



OcNOS®

**Open Compute
Network Operating System for Data Centers
Version 6.4.2**

Multicast Guide
December 2023

© 2023 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.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
<http://www.ipinfusion.com/>

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

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	ix
IP Maestro Support	ix
Audience	ix
Conventions	ix
Chapter Organization	ix
Related Documentation	ix
Migration Guide	x
Feature Availability	x
Support	x
Comments	x
Command Line Interface	11
Overview	11
Command Line Interface Help	11
Command Completion	12
Command Abbreviations	12
Command Line Errors	12
Command Negation	13
Syntax Conventions	13
Variable Placeholders	14
Command Description Format	15
Keyboard Operations	15
Show Command Modifiers	16
String Parameters	19
Command Modes	19
Transaction-based Command-line Interface	21
Multicast Configuration Guide	23
CHAPTER 1 IGMP Configuration	25
IGMP Versions	25
IGMP Operation	25
Topology	26
IGMP Configuration	27
CHAPTER 2 IGMP Proxy Configuration	35
Terminology	35
Enabling IP Multicast Routing	37
Enabling Proxy upstream interface	37
Enabling Proxy downstream interface	37
Enabling Unsolicited report interval	39
CHAPTER 3 PIM Sparse Mode Configuration	43
Terminology	43
Data Flow from Source to Receivers in PIM-SM Network Domain	44
PIM-SM Configuration	46

Enabling IP Multicast Routing	46
Configuring Rendezvous Point Statically	47
Configure Rendezvous Point Dynamically Using Bootstrap Router Method	50
Anycast-RP Configuration	55
CHAPTER 4 PIM Dense Mode Configuration	59
Terminology	59
Configuration	59
Enabling IP Multicast Routing	60
Enabling PIM-DM	61
CHAPTER 5 IGMP Snooping Configuration	63
Configuration	63
CHAPTER 6 PIM-ECMP Redirect Configuration	67
Terminology	67
PIM-ECMP Configuration	68
Topology	68
Configure PIM Router-ID	69
Configure PIM ECMP Bundle	69
Bind PIM ECMP Bundle	70
CHAPTER 7 MSDP Configuration	75
Overview	75
Caching SA state	75
MSDP Mesh Group	75
MSDP Default Peer	76
Configure PIM-SM	76
Configure MSDP	76
CHAPTER 8 PIM-BFD Configuration	85
PIM-BFD Configuration	85
CHAPTER 9 PIM Sparse-Dense Mode Configuration	95
Configuration Steps	95
Enabling IP Multicast Routing	95
Enabling PIM-SMDM	95
Sparse Mode Operation versus Dense Mode Operation	96
Multicast Command Reference	103
CHAPTER 1 Multicast Commands	105
clear ip mroute	106
debug ip mrib	107
ip mroute	108
ip multicast route-limit	109
ip multicast ttl-threshold	110
ip multicast-routing	111
ipv6 mroute	112
show debugging ip mrib	113
show ip mroute	114

show ip mvif	117
show running-config interface multicast	119
snmp restart mribd	120
CHAPTER 2 L3 IGMP Multicast Commands	121
clear ip igmp	122
debug ip igmp	123
ip igmp	125
ip igmp access-group	126
ip igmp immediate-leave	127
ip igmp join-group	128
ip igmp last-member-query-count	129
ip igmp last-member-query-interval	130
ip igmp limit	131
ip igmp mroute-proxy	132
ip igmp offlink	133
ip igmp proxy-service	134
ip igmp proxy unsolicited-report-interval	135
ip igmp querier-timeout	136
ip igmp query-interval	137
ip igmp query-max-response-time	138
ip igmp ra-option	139
ip igmp robustness-variable	140
ip igmp ssm-map enable	141
ip igmp ssm-map static	142
ip igmp static-group	143
ip igmp startup-query-count	144
ip igmp startup-query-interval	145
ip igmp version	146
show debugging ip igmp	147
show ip igmp groups	148
show ip igmp interface	150
show ip igmp proxy	152
show ip igmp ssm-map	154
show running-config interface igmp	155
CHAPTER 3 L2 IGMP Snooping Multicast Commands	157
igmp snooping	158
igmp snooping fast-leave	159
igmp snooping mrouter	160
igmp snooping querier	161
igmp snooping report-suppression	162
igmp snooping static-group	163
show igmp snooping interface	164
show igmp snooping groups	166
show igmp snooping mrouter	169
show igmp snooping statistics	170

CHAPTER 4	PIMv4 Commands	171
	clear ip mroute	173
	clear ip msdp peer	175
	clear ip msdp sa-cache	176
	clear ip pim sparse-mode	177
	debug ip pim	178
	debug ip pim packet	179
	debug pim bfd	180
	debug ip pim timer assert	181
	debug ip pim timer bsr	182
	debug ip pim timer hello	183
	debug ip pim timer joinprune	185
	debug ip pim timer register	187
	ip msdp default-peer	188
	ip msdp mesh-group	189
	ip msdp originator-id	190
	ip msdp password	191
	ip msdp peer	192
	ip msdp sa	193
	ip pim	194
	ip pim accept-register	195
	ip pim anycast-rp	196
	ip pim bfd	197
	ip pim bfd all-interfaces	198
	ip pim bidir-enable	199
	ip pim bidir-offer-interval	200
	ip pim bidir-offer-limit	201
	ip pim bidir-neighbor-filter	202
	ip pim bind ecmp-bundle	203
	ip pim bsr-border	204
	ip pim bsr-candidate	205
	ip pim cisco-register-checksum	206
	ip pim crp-cisco-prefix	207
	ip pim dr-priority	208
	ip pim ecmp-bundle	209
	ip pim exclude-genid	210
	ip pim hello-holdtime	211
	ip pim hello-interval	212
	ip pim ignore-rp-set-priority	213
	ip pim jp-timer	214
	ip pim neighbor-filter	215
	ip pim passive	216
	ip pim propagation-delay	217
	ip pim redundancy	218
	ip pim register-rate-limit	219
	ip pim register-rp-reachability	220
	ip pim register-source	221

ip pim register-suppression	222
ip pim router-id	223
ip pim rp-address	224
ip pim rp-candidate	226
ip pim rp-register-kat	227
ip pim spt-threshold	228
ip pim ssm	229
ip pim state-refresh origination-interval	230
ip pim unicast-bsm	231
show debugging ip pim	232
show debugging pim	233
show ip msdp peer	234
show ip msdp sa-cache	235
show ip pim interface	237
show ip pim interface df	239
show ip pim mroute	240
show ip pim neighbor	242
show ip pim nexthop	245
show ip pim bsr-router	246
show ip pim local-members	248
show ip pim rp-hash	249
show ip pim rp mapping	250
snmp restart pim	251
Index	253

Preface

This guide describes how to configure OcNOS.

IP Maestro Support

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

Audience

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

Conventions

[Table P-1](#) shows the conventions used in this guide.

Table P-1: Conventions

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

Chapter Organization

The chapters in command references are organized as described in [Command Description Format](#).

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

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

Related Documentation

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

Migration Guide

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

Feature Availability

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

Support

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

Comments

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

Command Line Interface

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

Overview

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

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

Command Line Interface Help

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

```
> show ?
```

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

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

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

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

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

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

Command Completion

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

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

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

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

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

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

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

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

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

Command Abbreviations

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

```
> sh 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 P-2](#) describes the conventions used to represent command syntax in this reference.

Table P-2: Syntax conventions

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

Table P-2: Syntax conventions (Continued)

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

Variable Placeholders

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

Table P-3: Variable placeholders

Token	Description
WORD	A contiguous text string (excluding spaces)
LINE	A text string, including spaces; no other parameters can follow this parameter
IFNAME	Interface name whose format varies depending on the platform; examples are: eth0, Ethernet0, ethernet0, xe0
A.B.C.D	IPv4 address
A.B.C.D/M	IPv4 address and mask/prefix
X:X::X:X	IPv6 address
X:X::X:X/M	IPv6 address and mask/prefix
HH:MM:SS	Time format
AA:NN	BGP community value
XX:XX:XX:XX:XX:XX	MAC address
<1-5> <1-65535> <0-2147483647> <0-4294967295>	Numeric range

Command Description Format

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

Table P-4: Command descriptions

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

Keyboard Operations

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

Table P-5: Keyboard operations

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

Table P-5: Keyboard operations (Continued)

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

Show Command Modifiers

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

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

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

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

Begin Modifier

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

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

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

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



```

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

```

Include Modifier

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

```

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

```

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

```

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

```

Exclude Modifier

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

```

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

```

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

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

Redirect Modifier

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

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

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

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

Last Modifier

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

For example:

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

String Parameters

The restrictions in [Table P-6](#) apply for all string parameters used in OcnOS commands, unless some other restrictions are noted for a particular command.

Table P-6: String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	“?”, “,”, “>”, “ ”, and “=” The “ ” is allowed only for <code>description</code> CLI 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 P-7: Common command modes

Name	Description
Executive mode	Also called <i>view</i> 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 <code>show</code> , <code>exit</code> , <code>quit</code> , <code>help</code> , and <code>enable</code> .
Privileged executive mode	Also called <i>enable</i> mode, in this mode you can run additional basic commands such as <code>debug</code> , <code>write</code> , and <code>show</code> .
Configure mode	Also called <i>configure terminal</i> 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.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

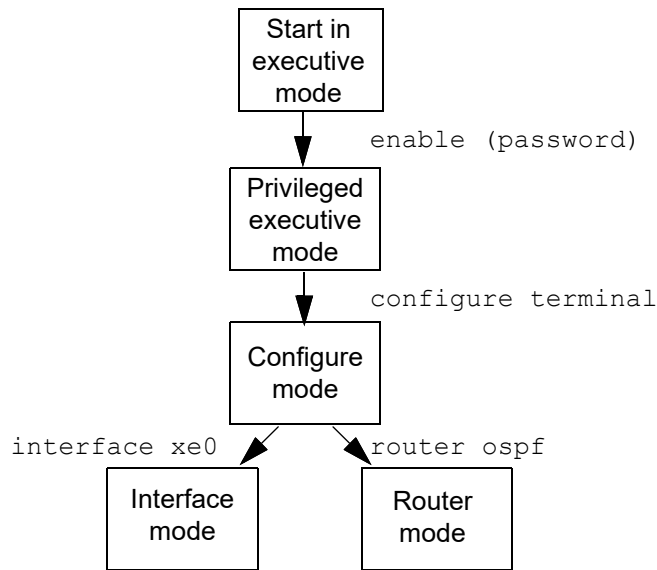


Figure P-1: Common command modes

To change modes:

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

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

```

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

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

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.

Multicast Configuration Guide

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](#).

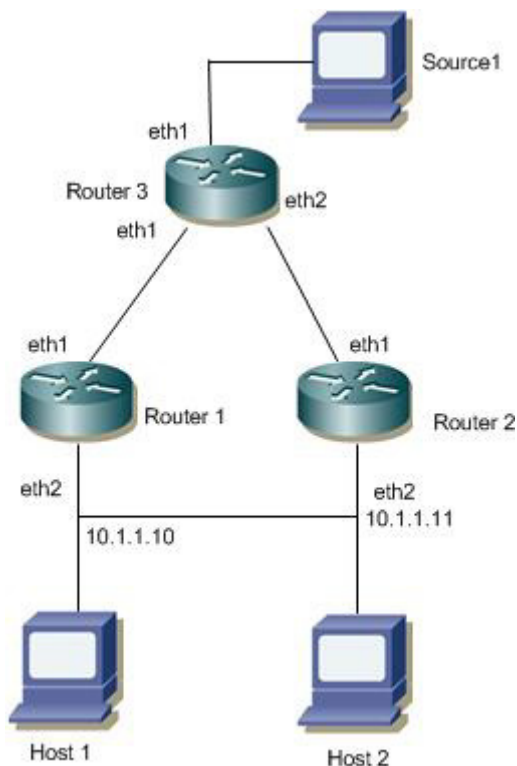


Figure 1-1: IGMP Topology

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)#exit	Exit interface mode.
(config)#exit	Exit Configure mode.

Validation

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

```
#show running-config
!
no service password-encryption
```

```

!
hostname rtr1
!
ip multicast-routing
!
!
interface eth2
ip address 10.1.1.10/24
no shutdown
ip igmp version 2

```

Configuring IGMP Parameters

The configuration that follows shows how IGMP parameters can be configured.

#configure terminal	Enter configure mode.
(config)#ip multicast-routing	Enable IP multicast routing
(config)#interface eth2	Enter interface mode
(config-if)#ip igmp access-group 1	Configures a access-list policy to control the multicast groups that hosts on the subnet serviced by an interface can join.
(config-if)#ip igmp immediate-leave group-list 1	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
(config-if)#ip igmp join-group 224.1.1.1	Statically binds a multicast group to the outgoing interface
(config-if)#ip igmp last-member-query-count 7	Sets the query count used when the software starts up.
(config-if)#ip igmp last-member-query-interval 25500	Sets the query interval used when the software starts up.
(config-if)#ip igmp limit 100	Configure Max Allowed State on this interface
(config-if)#ip igmp querier-timeout 300	Sets the querier timeout that the router uses when deciding to take over as the querier.
(config-if)#ip igmp query-interval 200	Sets the frequency at which the router sends IGMP host query messages.
(config-if)#ip igmp query-max-response-time 150	Sets the response time advertised in IGMP queries.
(config-if)#ip igmp ra-option	Enable ra-option.
(config-if)#ip igmp robustness-variable 4	Sets the robustness variable.
(config-if)#ip igmp startup-query-count 4	Sets the query count used when the router starts up.
(config-if)#ip igmp startup-query-interval 50	Sets the query interval used when the router starts up.
(config-if)#ip igmp static-group 225.1.1.1	Statically binds a multicast group to the outgoing interface.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit Configure mode.

Validation

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

```
Rtr1#show running-config
!
no service password-encryption
!
hostname rtr1
!
!
ip multicast-routing
!
!
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2
!!
```

```
Rtr1#show ip igmp interface eth2
Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Configured for version 2
Internet address is 10.1.1.10
IGMP interface limit is 100
IGMP interface has 2 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 0, v2-leaves: 0
v3-reports: 0
IGMP query interval is 200 seconds
IGMP Startup query interval is 50 seconds
IGMP Startup query count is 4
IGMP querier timeout is 300 seconds
IGMP max query response time is 150 seconds
Group Membership interval is 950 seconds
IGMP Last member query count is 7
Last member query response interval is 25500 milliseconds
```

Here is the sample configuration on Router-1 with all the IGMP related commands configured.

```
Rtr1#show running-config
!
no service password-encryption
!
hostname rtr1
!
!
```

IGMP Configuration

```
ip domain-lookup
!
ip multicast-routing
!
ip pim register-rp-reachability
ip pim crp-cisco-prefix
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.57/32 secondary
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.179/24
 no shutdown
!
interface eth1
 ip address 192.168.1.27/24
 no shutdown
 ip igmp version 2
!
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2

!
line con 0
 login
line vty 0 16
 exec-timeout 0 0
 login
line vty 17 39
 login
!
End
```

IGMP Group Table after IGMPV2 Membership Report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface.

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

Table 1-1: 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        Last Reporter
224.0.1.3          eth2           00:10:06     00:03:43      10.1.1.52
224.1.1.1          eth2           01:54:53     static         0.0.0.0
225.1.1.1          eth2           00:17:22     static         0.0.0.0
```

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

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

```
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:10:06
Group mode:     Exclude (Expires: 00:03:43)
State: Active
Last reporter:  10.1.1.52
Source list is empty
```

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

```
Interface:      eth2
Group:          224.1.1.1
Flags:          L
Uptime:         01:54:59
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty
```

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

```
Interface:      eth2
Group:          225.1.1.1
```

```

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

IGMP Group Table after IGMPV3 Membership report is received

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

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

Table 1-2: 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.

IGMP-Proxy Configuration Steps

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

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

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

Unicast routing protocol should be configured in the PIM domain.

Topology

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

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

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

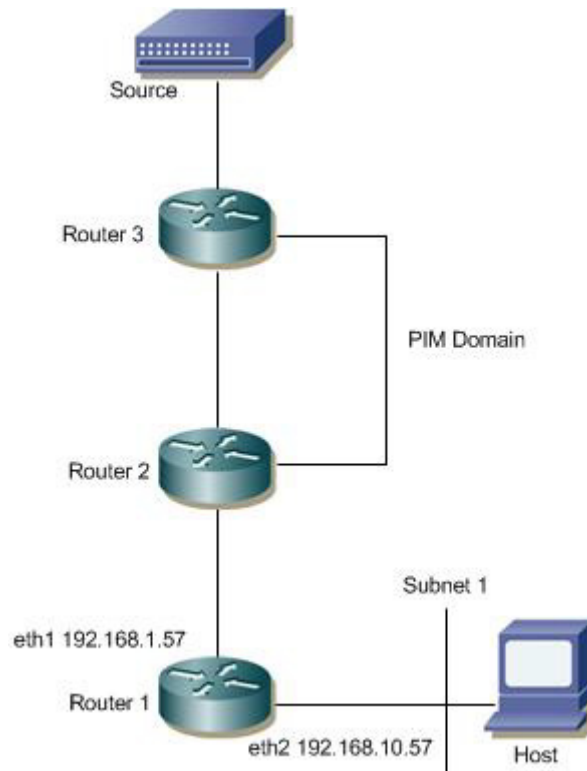


Figure 2-2: IGMP Proxy Topology

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)#exit	Exit Configure mode.

Enabling Proxy upstream interface

Enable IGMP proxy service on the interface in which the interface is in the direction toward the root of the multicast forwarding tree. In this example eth1 is the upstream interface which acts as an IGMP host.

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 192.168.1.57/24	Assign IP address to an interface
(config-if)#ip igmp proxy-service	Enable IGMP proxy service on the upstream interface.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit Configure mode.

Enabling Proxy downstream interface

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

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

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface lo
!!
ip multicast-routing
!
interface eth0
!
interface eth1
 ip address 192.168.1.57/24
 no shutdown
 ip igmp proxy-service
!
interface eth2
 ip address 192.168.10.57/24
 no shutdown
 ip igmp mroute-proxy eth1
!
```

IGMP proxy interface

The following output displays the IGMP Proxy interface information.

```
Router1#show ip igmp interface
```

```
Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 1000 milliseconds

Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Version 3 (default)
 IGMP mroute-proxy interface is eth1
 Internet address is 192.168.10.57
 IGMP interface has 1 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 1, v2-leaves: 0
v3-reports: 0
IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP Last member query count is 2
 Last member query response interval is 1000 milliseconds
```

IGMP proxy

The following output displays the IGMP proxy information.

```
Router1#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1
```

IGMP proxy groups

The following output displays the IGMP proxy group membership information.

```
Router1#show ip igmp proxy groups

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

IP Multicast Routing Table

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

```
Router1#show ip mroute

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

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

Enabling Unsolicited report interval

Enable IGMP proxy unsolicited report interval on the upstream interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time.

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip igmp proxy unsolicited-report-interval 20000	Enable IGMP proxy unsolicited report interval value on the upstream interface.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface eth0
!
interface eth1
ip address 192.168.1.57/24
ip igmp proxy-service
ip igmp proxy unsolicited-report-interval 20000
!
interface eth2
ip address 192.168.10.57/24
ip igmp mrouter-proxy eth1
!
interface lo
!
!
ip multicast-routing
!
```

IGMP proxy Unsolicited report interval

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

```
Router1#show ip igmp interface eth1

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

IGMP proxy group with unsolicited report interval

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

```
Router1#show ip igmp proxy groups

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

IP Multicast Routing Table

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

```
Router1#show ip mroute

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



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

CHAPTER 3 PIM Sparse Mode Configuration

The Protocol Independent Multicasting-Sparse Mode (PIM-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps geographically dispersed network nodes to conserve bandwidth and reduce traffic by simultaneously delivering a single stream of information to multiple locations. PIM-SM uses the IP multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topology-gathering protocol to populate a multicast routing table with routes.

Terminology

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

Rendezvous Point

A Rendezvous Point (RP) router is configured as the root of a non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP. Data from senders is sent to the RP so that receivers can discover who the senders are, and receive traffic destined for the group.

Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB decides where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link, once in each direction.

Tree Information Base

The Tree Information Base (TIB) is a collection of states at a PIM router storing the state of all multicast distribution trees at that router. The TIB is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

Upstream

Upstream indicates that traffic is going towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Downstream indicates that traffic is going away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In Source-Based Trees, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric used is `hop counts`, the branches of the multicast Source-Based Trees are minimum hop. If the metric used is `delay`, the branches are minimum delay. A corresponding multicast tree directly connects the source to all receivers for every multicast source. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces -- the source address and the multicast group.

Shared Trees

Shared trees, or RP trees (RPT), rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists. The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, then multicast to the members. This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

Note: Not all hosts are receivers.

Bootstrap Router

When a new multicast sender starts sending data packets, or a new receiver starts sending Join messages towards the RP for that multicast group, the sender needs to know the next-hop router towards the RP. The bootstrap router (BSR) provides group-to-RP mapping information to all the PIM routers in a domain, allowing them to map to the correct RP address.

Data Flow from Source to Receivers in PIM-SM Network Domain

1. Sending out Hello Messages

PIM routers periodically send Hello messages to discover neighboring PIM routers. Hello messages are multicast using the address, `224.0.0.13` (`ALL-PIM-ROUTERS` group). Routers do not send any acknowledgement that a Hello message was received. A `holdtime` value determines the length of time for which the information is valid. In PIM-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

2. Electing a Designated Router

In a multi-access network with multiple routers connected, one of the routers is selected to act as a designated router (DR) for a given period. The DR is responsible for sending Join/Prune messages to the RP for local members.

3. Determining the Rendezvous Point

PIM-SM uses a BSR to originate bootstrap messages, and to disseminate RP information. The messages are multicast to the group on each link. If the BSR is not apparent, the routers flood the domain with advertisements.

The router with the highest priority (if priorities are same, the higher IP address applies) is selected to be the RP. Routers receive and store bootstrap messages originated by the BSR. When a DR gets a membership indication from IGMP for (or a data packet from) a directly connected host, for a group for which it has no entry, the designated router (DR) maps the group address to one of the candidate RPs that can service that group. The DR then sends a Join/Prune message towards that RP. In a small domain, the RP can also be configured statically.

4. Joining the Shared Tree

To join a multicast group, a host sends an IGMP message to its upstream router, after which the router can accept multicast traffic for that group. The router sends a Join message to its upstream PIM neighbor in the direction of the RP. When a router receives a Join message from a downstream router, it checks to see if a state exists for the group in its multicast routing table. If a state already exists, the Join message has reached the shared tree, and the interface from which the message was received is entered in the Outgoing Interface list. If no state exists, an entry is created, the interface is entered in the Outgoing Interface list, and the Join message is again sent towards the RP.

5. Registering with the RP

A DR can begin receiving traffic from a source without having a Source or a Group state for that source. In this case, the DR has no information on how to get multicast traffic to the RP through a tree. When the source DR receives the initial multicast packet, it encapsulates it in a Register message, and unicasts it to the RP for that group. The RP de-encapsulates each Register message, and forwards the extracted data packet to downstream members on the RPT. Once the path is established from the source to the RP, the DR begins sending traffic to the RP as standard IP multicast packets, as well as encapsulated within Register messages. The RP temporarily receives packets twice. When the RP detects the normal multicast packets, it sends a Register-Stop message to the source DR, meaning it should stop sending register packets.

6. Sending Register-Stop Messages

When the RP begins receiving traffic from the source, both as Register messages and as unencapsulated IP packets, it sends a Register-Stop message to the DR. This notifies the DR that the traffic is now being received as standard IP multicast packets on the SPT. When the DR receives this message, it stops encapsulating traffic in Register messages.

7. Pruning the Interface

Routers attached to receivers send Prune messages to the RP to disassociate the source from the RP. When an RP receives a Prune message, it no longer forwards traffic from the source indicated in the Prune message. If all members of a multicast group are pruned, the IGMP state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

8. Forwarding Multicast Packets

PIM-SM routers forward multicast traffic onto all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork, and have a Time to Live (TTL) of one (1). The router performs an RPF check, and forwards the packet. If a downstream router has sent a join to this router or is a member of this group, then traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers.

PIM-SM Configuration

PIM-SM is a soft-state protocol. The required steps to configure PIM-SM are the following:

- Enable IP multicast on each PIM router (see [Enabling IP Multicast Routing](#))
- Enable PIM-SM on the desired interfaces (see [Enable PIM-SM on an Interface](#))
- Configure the RP statically (see [Configuring Rendezvous Point Statically](#)) or dynamically (see [Configure Rendezvous Point Dynamically Using Bootstrap Router Method](#)) depending on which method you use)

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

This section provides the steps to configure the PIM-SM feature. Configuration steps and examples are used for two relevant scenarios.

Topology

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

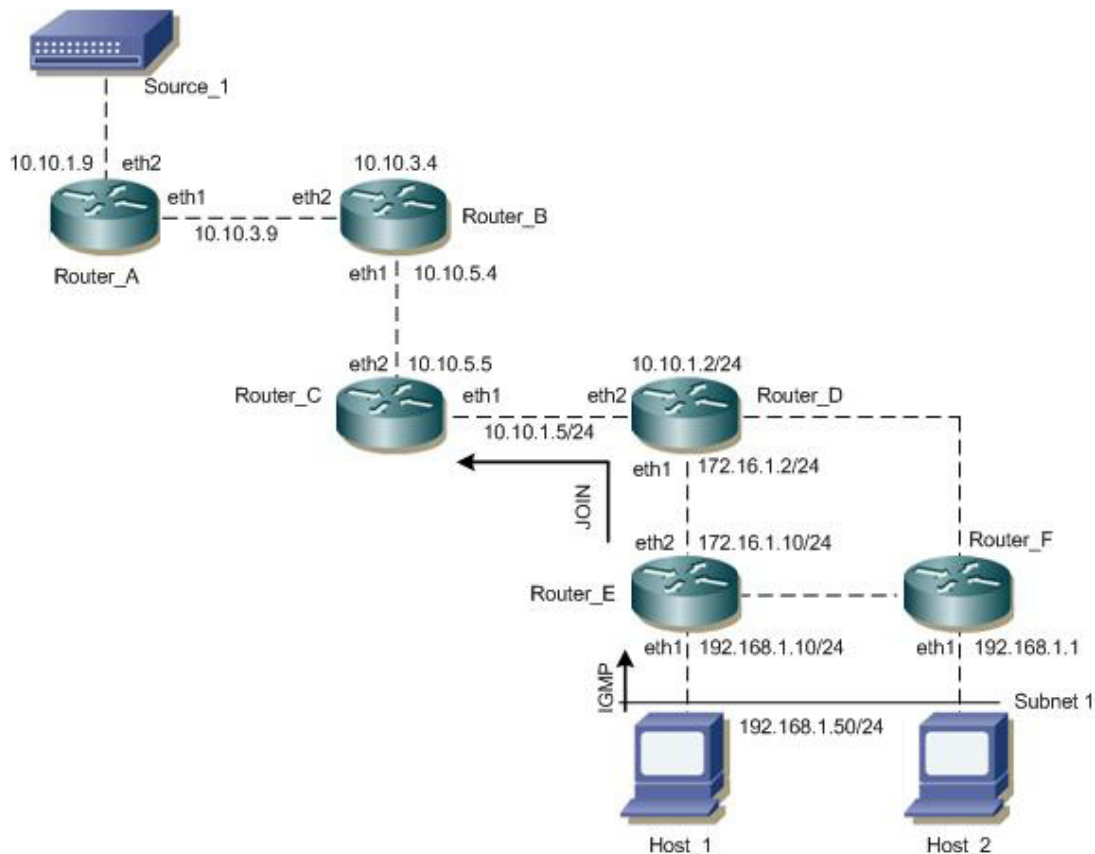


Figure 3-3: PIM-SM Topology

Enabling IP Multicast Routing

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

Enable IP Multicast Routing

#configure terminal	Enter configure mode.
(config)#ip multicast-routing	Enable IP multicast routing.
(config)#exit	Exit Configure mode.

Enable PIM-SM on an Interface

Enable PIM-SM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SM on the router.

#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured and Enter interface mode.
(config-if)#ip address 10.10.12.11/24	Configure the IP address for eth1.
(config-if)#ip pim sparse-mode	Enable PIM sparse mode on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured and Enter interface mode.
(config-if)#ip address 10.10.13.11/24	Configure the IP address for eth2.
(config-if)#ip pim sparse-mode	Enable PIM sparse mode on the interface.
(config-if)#exit	Exit interface mode.

Configuring Rendezvous Point Statically

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address with in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in [Figure 3-3](#), Router_C is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to Subnet 1. Two routers are attached to Subnet 1, Router_E and Router_F; both have default DR priority on eth1.

Since Router_E has a higher IP address on interface eth1, it becomes the Designated Router, and is responsible for sending Join messages to the RP (Router_C).

Configure Static RP

#configure terminal	Enter configure mode.
(config)#ip pim rp-address 10.10.1.5	Statically configure an RP address for multicast groups.
(config)#exit	Exit Configure mode.

Here is the sample configuration for Router_D:

```
hostname Router_D
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing

ip pim rp-address 10.10.1.5
!
```

Validation

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

RP Details

At Router_D, the show ip pim rp mapping command shows that 10.10.1.5 is the RP for all multicast groups 224.0.0.0/4, and is statically configured. All other routers will have a similar output:

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

Group(s): 224.0.0.0/4, Static
  RP: 10.10.1.5
  Uptime: 00:19:31
R-D#
```

Override RP cnt: 0At Router_D, use the show ip pim rp-hash command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.1.5
```


Interface Details

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

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

IP Multicast Routing Table

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

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

```
R-E#show ip pim mroute
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
Local      i.....
Joined     .....
Asserted   .....
FCR:

R-E#
```

At Router_E, eth2 is the incoming interface of the (*, G) entry, and eth1 is on the outgoing interface list of the (*, G) entry. This means that there is a group member through eth1, and the RP is reachable through eth2.

The 0 position on this 32-bit index is for eth1 (as illustrated in the interface display above). The j on the 0 index indicates that the Join has come from eth1.

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

```
R-C#show ip pim mroute
IP Multicast Routing Table

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

(*, 224.0.1.3)
```

```
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  Local      .....
  Joined    j.....
  Asserted  .....
FCR:

R-C#
```

Configure Rendezvous Point Dynamically Using Bootstrap Router Method

A static RP configuration works for a small, stable PIM network domain; however, it is not practical for a large and/or complex one. In such a network, if the RP fails or you have to change the assignment of the RP, you are required to reconfigure the static configurations on all PIM routers. Also, if you have several multicast groups mapped to several RPs, there are many repetitive configurations you are required to perform, which can be time consuming and laborious. Thus when it comes configuring RP in large and/or complex networking environments, configuring it dynamically is the best and most scalable method to use. Bootstrap router (BSR) configuration is one method of configuring the RP dynamically.

The BSR mechanism in a PIM domain uses the concept of a RP as a way for receivers to discover the sources that send to a particular multicast group. The BSR mechanism gives a way for a multicast router to learn the set of group-to-RP mappings required in order to function. The BSR's function is to broadcast the RP set to all routers in the domain.

Some of the PIM routers within a PIM domain are configured as Candidate-RPs (C-RPs). A subset of the C-RPs is eventually used as the actual RPs for the domain. An RP configured with a lower value in the priority field has a higher priority.

Some of the PIM routers in the domain are configured to be Candidate-BSRs (C-BSR). One C-BSR is selected to be the BSR for the domain, and all PIM routers in the domain learn the result of this election through Bootstrap messages (BSM). The C-BSR with highest value in the priority field is elected to be the BSR. The C-RPs then report their candidacies to the elected BSR, which chooses a subset of the C-RPs, and distributes corresponding group-to-RP mappings to all the routers in the domain using Bootstrap messages.

This section provides 2 examples to illustrate the BSR configuration for configuring RP dynamically.

Example 1

For this example, refer to Figure 1 for the topology.

To dynamically configure the RP, `Router_C` on `eth1` and `Router_D` on `eth1` are configured as a Candidate RP using the `ip pim rp-candidate` command. `Router_D` on `eth1` is also configured as the Candidate BSR. Since no other router has been configured as the candidate BSR, `Router_D` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

The highest priority router (configured with lowest priority value) is chosen as the RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the RP to ensure that all routers in the PIM-domain have the same RP for the same group.

To change the default priority of any candidate RP, use the `ip pim rp-candidate IFNAME PRIORITY` command. At `Router_D`, the `show ip pim rp mapping` command shows that `Router_C` is chosen as the RP for a specified group.

Configure RP Dynamically for Router C

#configure terminal	Enter configure mode.
(config)#ip pim rp-candidate eth1 priority 2	Give this router the candidate RP status using the IP address of the specified interface.

Configure RP Dynamically for Router D

#configure terminal	Enter configure mode.
(config)#ip pim bsr-candidate eth1	Give this router the candidate BSR status using the name of the interface.
(config)#ip pim rp-candidate eth1 priority 2	Give this router the candidate RP status using the IP address of the specified interface.

The following output displays the complete configuration at Router_C and Router_D:

```
Router_D#show running-config
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
ip multicast-routing
ip pim bsr-candidate eth1
ip pim rp-candidate eth1 priority 2
!

Router_C#show running-config
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
ip pim rp-candidate eth1
```

Validation

This section provides the steps to verify the RP configuration.

PIM Group-to-RP Mappings

The `show ip pim rp mapping` command displays the group-to-RP mapping details and displays information about RP candidates. There are two RP candidates for the group range, 224.0.0.0/4. RP Candidate 10.10.1.5 has a default priority of 192, whereas, RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as RP for the multicast group, 224.0.0.0/4.

```
R-D#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
    Uptime: 00:02:24, expires: 00:02:11
  RP: 10.10.1.5
    Info source: 10.10.1.5, via bootstrap, priority 2
    Uptime: 00:02:26, expires: 00:02:06
Override RP cnt: 0
```

```
Group(s): 224.0.0.0/4, Static
  RP: 10.10.1.5
    Uptime: 00:55:25
```

R-D#

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
  RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

After RP information reaches all PIM routers in the domain, various state machines maintain all routing states, as a result of Join/Prune from group membership. To display information on interface details and the multicast routing table, refer to the *Configuring Rendezvous Point Statically* section.

Example 2

To dynamically configure the RP, Router_2 on eth1 is configured as a Candidate RP using the `ip pim rp-candidate` command. Since no other router is configured as C-RP, Router_2 becomes the RP. Router_1 on eth1 and Router_2 on eth1 are configured as the Candidate BSRs. Since Router_1 has a higher priority value than Router_2, Router_1 becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

Topology

For this example, refer to [Figure 3-4](#) for the topology.

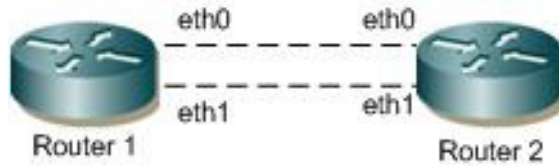


Figure 3-4: Bootstrap Router Topology

Configuration

Router 1

#configure terminal	Enter configure mode.
(config)#ip pim bsr-candidate eth1	Configure eth1 of Router 1 as C-BSR. The default priority is 64, so it is not necessary to designate a priority.
(config)#exit	Exit Configure mode.

Router 2

#configure terminal	Enter configure mode.
(config)#ip pim bsr-candidate eth1 10 25	Configure eth1 of Router 2 as C-BSR with a hash mask length of 10, and a priority of 25.
(config)#ip pim rp-candidate eth1 priority 0	Configure interface eth1 as C-RP with a priority of 0.
(config)#exit	Exit Configure mode.

Router 2 Unicast BSM

When the `ip pim unicast-bsm` command is configured on an interface that is a DR for a network, then that interface unicasts the stored copy of BSM to the new or rebooting router.

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ip pim dr-priority 10	Configure eth1 as DR
(config-if)#ip pim unicast-bsm	Enable sending and receiving of Unicast BSM for backward compatibility.
(config-if)#exit	Exit interface mode.

Validation

1. Verify the C-BSR state on Router 1.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 20.0.1.21
  Uptime:      00:01:39, BSR Priority: 64, Hash mask length: 10
  Next bootstrap message in 00:00:53
  Role: Candidate BSR
```

State: Elected BSR

2. Verify the C-BSR state on Router 2.

The initial state of C-BSR is P-BSR before transitioning to C-BSR. The two states are illustrated in the sample outputs from the `show ip pim bsr-router` command below.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 20.0.1.21
  Uptime:      00:02:39, BSR Priority: 64, Hash mask length: 10
  Expires:     00:00:03
  Role: Candidate BSR
  State: Pending BSR
```

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 20.0.1.21
  Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
  Expires:     00:02:07
  Role: Candidate BSR
  State: Candidate BSR
Candidate RP: 20.0.1.11(eth2)
  Advertisement interval 60 seconds
  Next C-RP advertisement in 00:00:02
  Backoff cnt 1
```

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 20.0.1.11
    Info source: 20.0.1.21, via bootstrap, priority 0
    Uptime: 00:02:17, expires: 00:02:26
Override RP cnt: 0
```

3. Verify RP-set information on E-BSR.

```
R1#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 20.0.1.11
    Info source: 20.0.1.11, via bootstrap, priority 0
    Uptime: 00:00:22, expires: 00:02:12
Override RP cnt: 0
```

4. Verify RP-set information on C-BSR.

```
ARP1#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Anycast-RP 1.1.1.152 members :
  4.4.4.5   7.7.7.1   23.23.23.1
```

```
Group(s): 224.0.0.0/4, Static
  RP: 1.1.1.152
    Uptime: 00:00:37
ARP1#
```

Anycast-RP Configuration

The Anycast-RP feature provides load balancing among active RPs and redundancy in a PIM-SM network domain. In a PM-SM configuration, only a single active RP for each multicast group within a domain is permitted. However, in an Anycast-RP configuration, this restriction is removed with the support of multiple active RPs for each group in a domain.

OcNOS supports Anycast-RP using the PIM implementation. In PIM Anycast-RP, Multicast Source Discovery Protocol (MSDP) is not employed to share information about active sources. Instead the Register mechanism in PIM is extended to provide this same function.

The following describes Anycast-RP in PIM-SM:

- A Unicast IP address is used as the RP address. The address is statically configured, and associated with all PIM routers throughout the domain.
- A set of routers in the domain is chosen to act as RPs for this RP address. These routers are called the Anycast-RP set.
- Each router in the Anycast-RP set is configured with a loopback address. The loopback address is configured on all RPs for the loopback interface, then configured as the RP address (static RP), and injected into OSPF using redistribute connected. The PIM-SM implementation uses only the first non-loopback address configured on the loopback interface. Therefore, it is important to be sure that the Anycast-RP address is configured with the first non-loopback address.
- Each router in the Anycast-RP set also needs a separate IP address, which is used for communication between the RPs.
- The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.
- Each router in the Anycast-RP set is configured with the addresses of all other routers in the Anycast-RP set. This must be consistently configured in all RPs in the set.h

Topology

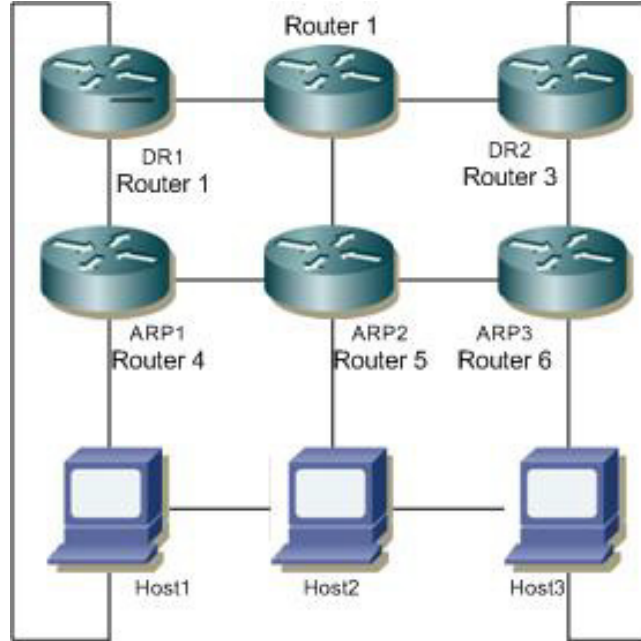


Figure 3-5: Anycast RP Topology

Host1 and Host3 act as hosts and sources for sending join and multicast data packets; Host2 acts as a host.

ARP1, ARP2 and ARP3

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter the loopback interface.
(config-if)#ip address 1.1.1.152/32 secondary	Configure the IP address for loopback
(config-if)#exit	Exit the Configure mode.
(config)#ip pim rp-address 1.1.1.152	Configure the static RP with the address of the loopback.
(config)#ip pim anycast-rp 1.1.1.152 4.4.4.5	Configure the member RP address. In this example, 4.4.4.5 is the member RP in ARP2. It is the address used for communication between all RPs.
(config)#ip pim anycast-rp 1.1.1.152 7.7.7.1	Configure the member RP address. In this example, 7.7.7.1 is the member RP in ARP3. It is the address used for communication between all RPs.
(config)#ip pim anycast-rp 1.1.1.152 23.23.23.1	Configure the member RP address. In this example, 23.23.23.1 is the member RP in ARP1. It is the address used for communication between all RPs.
(config)#exit	Exit the Configure mode.

Disable Anycast-RP

#configure terminal	Enter configure mode.
(config)#no ip pim anycast-rp 1.1.1.152	Disable Anycast-RP.

(config)#no ip pim rp-address 1.1.1.152	Disable static RP.
(config)#exit	Exit Configure mode.

Validation

1. Verify RP-mapping in ARP1.

```
#show ip pim rp mapping
  PIM Group-to-RP Mappings
  Override RP cnt: 0
  Anycast-RP 1.1.1.152 members:23.23.23.1
  Group(s): 224.0.0.0/4, Static
  RP: 1.1.1.152
    Uptime: 00:00:13s
```

2. Verify RP-mapping in ARP1 after disabling anycast-RP and RP-address.

```
ARP1#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Anycast-RP 1.1.1.152 members :
 4.4.4.5   7.7.7.1   23.23.23.1

Group(s): 224.0.0.0/4, Static
  RP: 1.1.1.152
    Uptime: 00:00:37
ARP1#
```

CHAPTER 4 PIM Dense Mode Configuration

Protocol Independent Multicast - Dense Mode (PIM-DM) is a data-driven multicast routing protocol that builds source-based multicast distribution trees that operate on the flood-and-prune principle. PIM-DM requires unicast-reachability information, but it does not depend on a specific unicast routing protocol.

Terminology

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

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only when `IF1` is the interface the router would use in order to reach `SourceA`. It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path to the network. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

Forwarding Multicast Packets

PIM-DM routers forward multicast traffic to all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers, if the downstream router is a member of this group.

Upstream

Upstream traffic is traffic that is going towards the source.

Downstream

Downstream traffic is anything other than the upstream interface for that group.

Nexthop

PIM-DM does periodic lookups for prefixes to check router reachability. The nexthop lookup mechanism avoids periodic lookup. During start-up, PIM-DM notifies NSM (Network Services Manager) about the prefixes that pertain to them. NSM notifies the protocols if a better nexthop is available, or if a nexthop becomes unavailable. In this way, PIM-DM does not expend resources to do periodic lookups, because NSM is proactive in their maintenance.

Configuration

Configuring PIM-DM requires the following steps:

- Enable IP multicast on each PIM router (see [Enabling IP Multicast Routing](#))

- Enable PIM-DM on the desired interfaces (see [Enabling PIM-DM](#))

This section provides the configuration steps for configuring PIM-DM and examples for a relevant scenario.

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

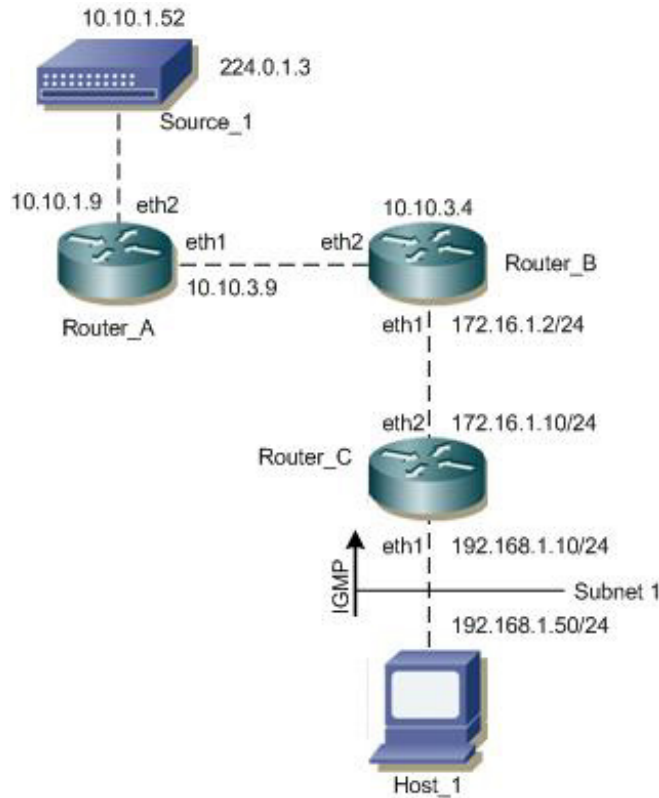


Figure 4-6: PIM-DM Configuration Topology

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

1. Host_1 sends an IGMP membership report to Subnet 1.
2. After Router_C receives this report, it associates its receiving interface, eth1, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches Router_C, it forwards via the interface, eth1, because there is a local member on this interface for this group. Router_C has a downstream receiver, so it does not send a prune message to its upstream neighbor router, Router_B.

Enabling IP Multicast Routing

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

#configure terminal	Enter configure mode.
(config)#ip multicast-routing	Enable IP multicast routing.
(config)#exit	Exit Configure mode.

Enabling PIM-DM

Enable PIM-DM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM.

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.10.15.12/24	Configure the IP address for eth1.
(config-if)#ip pim dense-mode	Enable PIM dense mode on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 10.10.14.12/24	Configure the IP address for eth1.
(config-if)#ip pim dense-mode	Enable PIM dense mode on the interface.
(config-if)#exit	Exit interface mode.

The following is a sample configuration for Router_C:

```

hostname Router_C
!
interface eth0
!
interface eth1
 ip pim dense-mode
!
interface eth2
 ip pim dense-mode
!
interface lo
!
!
ip multicast-routing
!
```

Validation

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

```

Router_C#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR
                  Mode     Count  prior
192.168.1.10     eth1      0      v2/D   0      1
172.16.1.10      eth2      2      v2/D   1      1
```

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

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
  Incoming interface: eth2
  Outgoing interface list:
    eth1 (1)
```

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

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table
(10.10.1.52, 224.0.1.3)
RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
Upstream IF: eth2
  Upstream State: Forwarding
  Assert State: NoInfo
Downstream IF List:
  eth1, in 'olist':
    Downstream State: NoInfo
    Assert State: NoInfo
```

CHAPTER 5 IGMP Snooping Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP) Snooping.

Note: Execute the `switchport` command on each port to change to Layer-2 mode.

Without IGMP, Layer-2 switches handle IP multicast traffic in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Only one membership report is relayed from a group, instead of a report from each host in the group. To achieve this, IGMP Snooping is enabled on the switches.

Topology

This example describes the configuration on switch S1. The eth1 interface is configured as a multicast router port.

Because IGMP Snooping is used in bridged LAN environments, router R1 does not require running IGMP Snooping, and can run any multicast protocol (such as PIM-SM). Thus, the configuration on R1 is not included in this example.

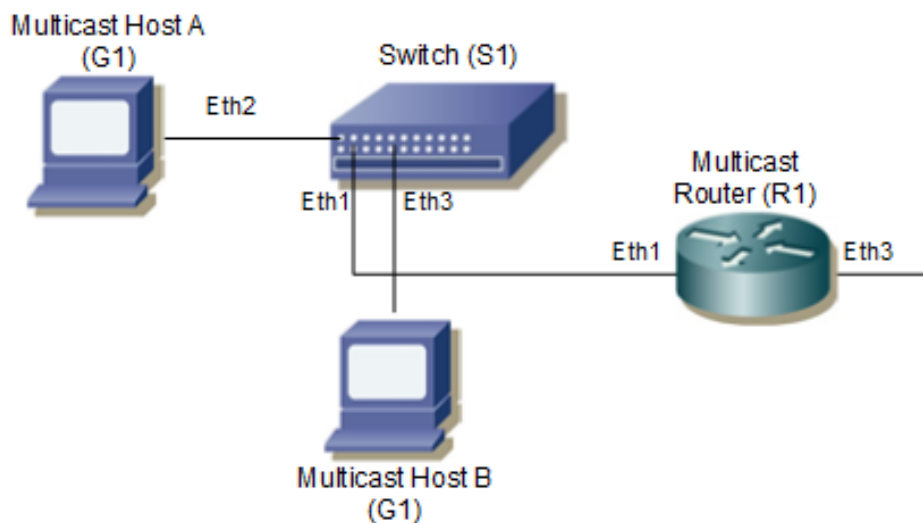


Figure 5-7: IGMP Snooping Topology

As a result of this configuration:

- The switch itself replies with membership report messages in response to queries received on interface eth1. However, if you do not enable report suppression on the switch, when it receives an IGMP Query message on eth1, it forwards it to both Host A and Host B. As a result, both hosts reply with a Membership report (as Layer-2 IGMP is running on the hosts).
- Because Host A and Host B are members of the same multicast group, the router is not notified when A leaves the group, because the group still has another member. When Host B leaves the group, the switch will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

Configuration

To enable IGMP Snooping on an interface:

1. Add a bridge to the spanning-tree table

2. Specify the interface to be configured
3. Associate the interface with bridge group
4. IGMP snooping will be enabled by default
5. Configure ports that are connected to routers as multicast router ports
6. By default, IGMP report suppression is enabled on the switch

S1

#configure terminal	Enter the Configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Add bridge 1 to the spanning-tree table.
(config)#vlan database	enter VLAN mode
(config-vlan)# vlan 2 bridge 1	Create VLAN and add it to bridge 1
(config)#exit	Exit VLAN mode
(config)#interface eth3	Specify the interface eth3 to be configured, and Enter interface mode.
(config-if)#shutdown	Shut down the interface.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate the interface eth1 with bridge-group 1 .
(config-if)#switchport mode trunk	Configure the port as an trunk port.
(config-if)#switchport trunk allowed vlan all	Add VLAN to trunk
(config-if)#no shutdown	Bring up the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify interface eth1 to be configured.
(config-if)#shutdown	Shut down the interface.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface eth1 with bridge-group 1.
(config-if)#switchport mode trunk	Configure the port as an trunk port.
(config-if)#switchport trunk allowed vlan all	Add VLAN to trunk
(config-if)#no shutdown	Bring up the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify interface eth2 to be configured.
(config-if)#shutdown	Shut down the interface.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface eth2 with bridge-group 1 .
(config-if)#switchport mode trunk	Configure the port as an trunk port.
(config-if)#switchport trunk allowed vlan all	Add VLAN to trunk
(config-if)#no shutdown	Bring up the interface.
(config-if)#exit	Exit interface mode.
(config)#interface vlan1.2	Specify interface vlan1.1 to be configured.
(config)#ip address 1.2.3.4/24	Specify IP address

(config-if)# igmp snooping mrouter interface eth1	Configure this port as a multicast router port
(config-if)#exit	Exit interface mode

Validation

```
#show running-config interface eth3
!
interface eth3
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show running-config interface eth1
!
interface eth1
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show running-config interface eth2
!
interface eth2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan Group/Source Address Interface Flags Uptime Expires Last Reporter Version
2 224.1.1.1 eth3 R 00:00:03 00:04:17 0.0.0.0 V3
2 224.1.1.1 eth2 R 00:00:03 00:04:17 0.0.0.0 V3

#show igmp snooping interface vlan1.2
IGMP Snooping information for vlan1.2
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 1
Number of Groups: 1
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 2
Active Ports:
Eth3
Eth1
```

Eth2

CHAPTER 6 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.

Note: PIM-ECMP feature is not supported for ZebIC.

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.

Upstream

Towards the root of the multicast forwarding tree. An upstream router refers to a router that is forwarding, or potentially capable of forwarding, data packets onto interfaces in an ECMP bundle. When there are multiple routers forwarding packets onto interfaces in the ECMP bundle, all these routers are called upstream routers.

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.

Sending 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 3, PIM Sparse Mode Configuration](#)

Topology

In this network topology, the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

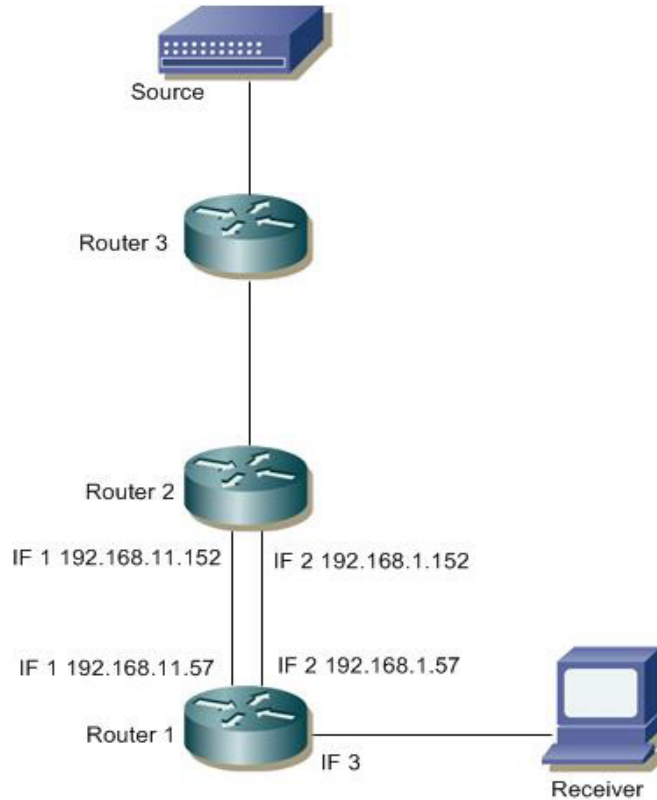


Figure 6-8: PIM ECMP Redirect Topology

Configure PIM Router-ID

Configure PIM router-id on all of the PIM routers inside the PIM domain:

# configure terminal	Enter configure mode.
(config)# ip pim router-id 1.1.1.1	Configure PIM router-id
(config)#exit	Exit Configure mode.

Validation

```
#show running-config
!
ip multicast-routing
!
ip pim router-id 1.1.1.1
```

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

```

PIM-ECMP Redirect Configuration

```
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

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 as an MSDP peer receives a SA message from its peer.

MSDP Mesh Group

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

MSDP Default Peer

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

Configure PIM-SM

For the MSDP topology in [Figure 7-9](#), you must enable PIM-SM on all the routers in both PIM domains and make RTR-1 a rendezvous point (RP) in Domain-1 and RTR-2 an RP in Domain-2. For the steps to configure PIM-SM and RPs, see [Chapter 3, PIM Sparse Mode Configuration](#).

Configure MSDP

In the topology in [Figure 7-9](#), 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

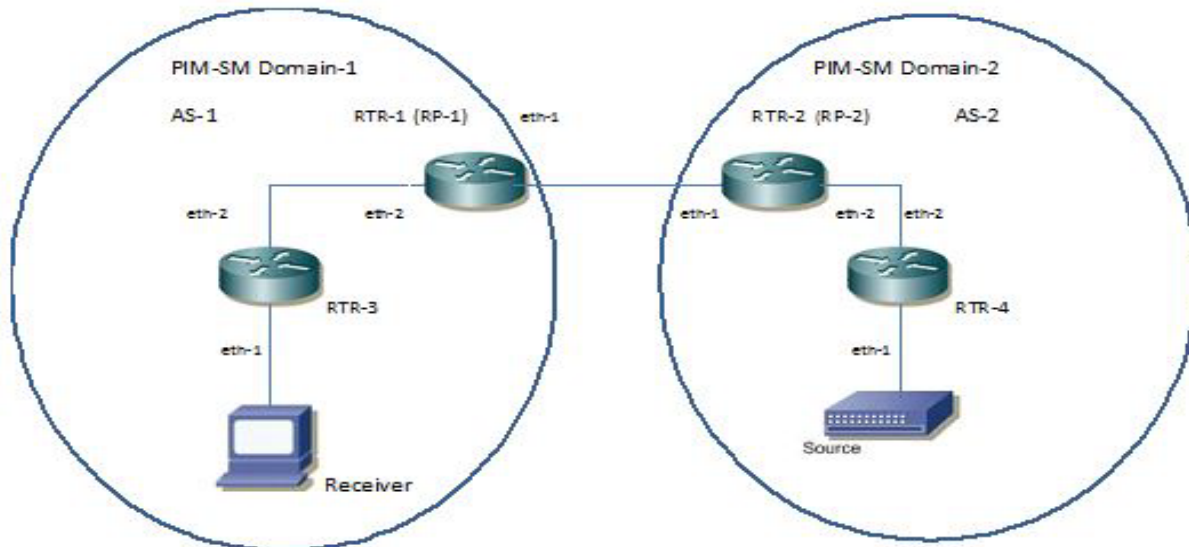


Figure 7-9: MSDP topology

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	Configure a MSDP peer.
--or--	
(config)#ip msdp peer 11.1.1.12 connect source eth1	Use the connect-source option to specify the primary IP address of the interface to use as the source IP address of the MSDP TCP connection.
(config)#ip msdp password myPass peer 11.1.1.12	Configure an MSDP password for the peer. You must specify the same command at RTR-2. The password must match at both the routers.
(config)#ip msdp default-peer 11.1.1.12	Configure MSDP default peer.
(config)#ip msdp mesh-group mesh1 11.1.1.12	Configure MSDP mesh group.
(config)#ip msdp originator-id eth2	Configure MSDP originator identifier.
(config)#exit	Exit configure mode.

Validation

RTR-1

```
#show running-config
!
!Last configuration change at 06:54:59 EDT Tue May 28 2019 by ocnos
!
no service password-encryption
!
hostname RTR1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
ssh login-attempts 0
ssh server port 39681568
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$wOL9u7T.$YENa7qmmntL3zWMXKBWSKw/
feature rsyslog
```

MSDP Configuration

```
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 bsr-candidate eth2
ip pim rp-candidate eth2
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.52.3/24
!
interface eth1
 ip address 11.1.1.11/24
 ip pim bsr-border
 ip pim sparse-mode
!
interface eth2
 ip address 10.1.1.11/24
 ip pim sparse-mode
!
interface eth3
 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
!
end
```

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 7-9](#), 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 - 1 entries
(20.1.1.11, 224.1.1.1), RP 12.1.1.12, 00:00:14/00:03:16
#

```

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      .....
  Joined     ..j.....
  Asserted   .....
FCR:

(20.1.1.10, 224.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 0
Upstream State: JOINED
  Local      .....
  Joined     .....
  Asserted   .....
  Outgoing   ..o.....

(20.1.1.10, 224.1.1.1, rpt)

```

MSDP Configuration

```
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
--More--  Local      .....
          Pruned    .....
          Outgoing  ..o.....
```

```
#sh ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(20.1.1.11, 224.1.1.1), RP 12.1.1.12, 00:00:14/00:03:16
#
```

RTR-2

```
#show running-config
!
!Last configuration change at 13:58:59 EDT Mon May 27 2019 by ocnos
!
no service password-encryption
!
hostname RTR2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$wOL9u7T.$YENa7qmmtL3zWMXKBWSKw/
feature rsyslog
ip msdp peer 11.1.1.11
ip msdp default-peer 11.1.1.11
ip msdp mesh-group mesh1 11.1.1.11
ip msdp password myPass peer 11.1.1.11
ip msdp originator-id eth2
!
ip multicast-routing
!
ip pim bsr-candidate eth2
ip pim rp-candidate eth2
!
interface lo
 ip address 127.0.0.1/8
```

```
--More--  ipv6 address ::1/128
mtu 65536
!
interface eth0
 ip address 192.168.52.2/24
!
interface eth1
 ip address 11.1.1.12/24
 ip pim bsr-border
 ip pim sparse-mode
!
interface eth2
 ip address 12.1.1.12/24
 ip pim sparse-mode
!
interface eth3
 shutdown
!
router ospf 200
 network 12.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
router bgp 2
 neighbor 11.1.1.11 remote-as 1
!
line con 0
 login
line vty 0 39
 login
!
end
```

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: 15
    Keepalive received: 17
#
```

RTR-3

```
#show running-config
!
!Last configuration change at 14:07:38 EDT Mon May 27 2019 by ocnos
!
no service password-encryption
```

MSDP Configuration

```
!  
hostname RTR3  
!  
logging monitor 7  
!  
ip vrf management  
!  
ip domain-lookup  
feature telnet  
ssh login-attempts 0  
ssh server port 40574496  
no feature ssh  
snmp-server enable snmp  
snmp-server view all .1 included  
feature ntp  
ntp enable  
username ocnos role network-admin password encrypted $1$wOL9u7T.$YENa7qmmtL3zWMXKBWSKw/  
feature rsyslog  
!  
ip multicast-routing  
!  
ip pim rp-address 10.1.1.11  
!  
interface lo  
  ip address 127.0.0.1/8  
  ipv6 address ::1/128  
  mtu 65536  
!  
interface eth0  
--More-- ip address 192.168.52.6/24  
!  
interface eth1  
  ip address 13.1.1.13/24  
  ip pim sparse-mode  
!  
interface eth2  
  ip address 10.1.1.13/24  
  ip pim sparse-mode  
!  
interface eth3  
  shutdown  
!  
interface eth4  
  shutdown  
!  
router ospf 100  
  network 10.1.1.0/24 area 0.0.0.0  
  cspf disable-better-protection  
!  
line con 0
```

```
login
line vty 0 39
  login
!
end
```

```
#sh ip igmp bgr
IGMP Connected Group Membership
Group Address      Interface          Uptime      Expires      State      Last Reporter
224.1.1.1          eth1              16:58:51    00:03:39    Active     13.1.1.11
#
```

RTR-4

```
#show running-config
!
!Last configuration change at 13:57:34 EDT Mon May 27 2019 by ocnos
!
no service password-encryption
!
hostname RTR4
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
ssh login-attempts 0
ssh server port 20761744
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$ypBh3Wo/$4Fq/DbkFF/UWeA7YnTYMm1
feature rsyslog
!
ip multicast-routing
!
interface lo
  ip address 127.0.0.1/8
  ipv6 address ::1/128
  mtu 65536
!
interface eth0
  ip address 192.168.52.5/24
!
--More-- interface eth1
```

MSDP Configuration

```
ip address 20.1.1.14/24
ip pim sparse-mode
!
interface eth2
ip address 12.1.1.14/24
ip pim sparse-mode
!
interface eth3
shutdown
!
router ospf 200
network 12.1.1.0/24 area 0.0.0.0
cspf disable-better-protection
!
line con 0
login
line vty 0 39
login
!
end
```

CHAPTER 8 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

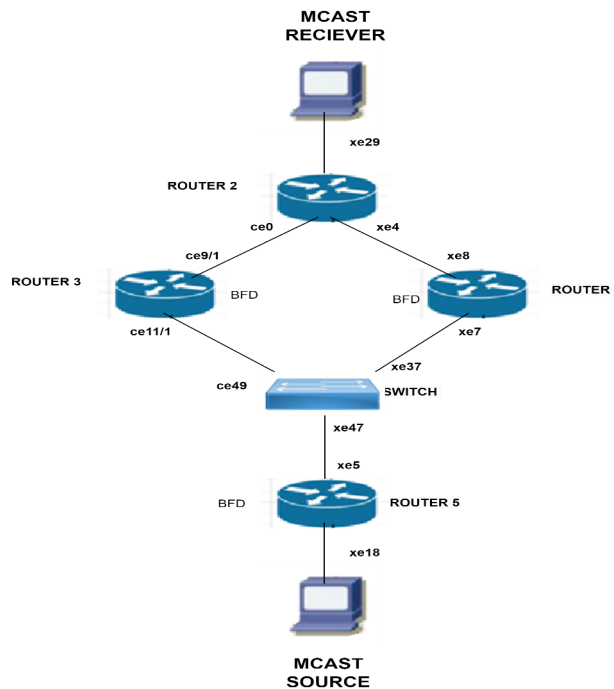


Figure: PIM-BFD Configuration Topology

Figure 8-10: 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.

ROUTER2

#configure terminal	Enter configuration mode.
OcNOS(config)#ip multicast-routing	Configure IP multicast routing

PIM-BFD Configuration

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

ROUTER3

#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)#int ce7/1	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

PIM-BFD Configuration

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

ROUTER4

#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) #int xe7	Entering interface ce7/1
OcNOS (config-if) #switchport	Configure Switchport
OcNOS (config-if) #bridge-group 1	Configure bridge group 1
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)#int 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)#int 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)#int 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

PIM-BFD Configuration

OcNOS (config-if)#exit	Exit interface mode.
OcNOS (config-if)#commit	Commit all the transactions

ROUTERS

#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

ROUTER2

```
#sh 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 /

```
#sh ip pim neighbor
```

```
Total number of PIM neighbors:2
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR 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

ROUTER3

```
#sh 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

```
#sh ip pim neighbor
```

```
Total number of PIM neighbors:3
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR 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

```
#sh bfd session
```

```
BFD process for VRF: (DEFAULT VRF)
```

```
=====
```

Sess-Idx	Remote-Disc	Lower-Layer	Sess-Type	Sess-State	UP-Time	Interface
258	NA	IPv6	Micro-BFD	Up	00:34:25	vlan1.120
						NA

```
fe80::eac5:7aff:fea8:7cb9/128
```

PIM-BFD Configuration

```

HW SESS: TYPE          INTERFACE          LOC_DISC  REM_DISC  LOCAL_STATE
=====
Single Hop  cell/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  cell/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  cell/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  cell/1          4         2052     Up

```

Number of Sessions: 4

ROUTER4

```
#sh 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

```
#sh bfd session
```

BFD process for VRF: (DEFAULT VRF)

```

=====
Sess-Idx  Remote-Disc  Lower-Layer  Sess-Type  Sess-State  UP-Time  Interface
Down-Reason Remote-Addr
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

ROUTER5

#sh 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 /

#sh ip pim neighbor

Total number of PIM neighbors:2

Neighbor Address	Interface	Uptime/Expires	Ver	DR 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

#sh bfd session

BFD process for VRF: (DEFAULT VRF)

```

=====
Sess-Idx  Remote-Disc  Lower-Layer  Sess-Type  Sess-State  UP-Time  Interface
Down-Reason Remote-Addr
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

#sh ipv6 mld groups detail

MLD Connected Group Membership Details

PIM-BFD Configuration

```
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
```

```
#sh 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

```
#sh bfd session
```

```
BFD process for VRF: (DEFAULT VRF)
```

```
=====
Sess-Idx  Remote-Disc  Lower-Layer  Sess-Type  Sess-State  UP-Time  Interface
Down-Reason  Remote-Addr
```

```
Number of Sessions:      0
```

CHAPTER 9 PIM Sparse-Dense Mode Configuration

PIM-SMDM is an integrated protocol which handles both sparse groups and dense groups at the same time. In sparse-dense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is sparse if the router knows about an RP for that group.

Note: PIM-SMDM is not supported for ZebIC releases.

Configuration Steps

The required steps to configure PIM-SMDM are the following:

- Enable IP multicast on each PIM router (see [Enabling IP Multicast Routing](#))
- Enable PIM-SMDM on the desired interfaces (see [Enabling PIM-SMDM](#))
- Example for the group operating in sparse-mode having Static RP (see [Configuring Rendezvous Point Statically for PIM-SMDM](#))
- Example for the group operating in dense-mode having no RP

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

This section provides the steps to configure the PIM-SMDM feature. Configuration steps and examples are used for two relevant scenarios. The following figure displays the network topology used in these examples:

Enabling IP Multicast Routing

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

#configure terminal	Enter configure mode.
(config)#ip multicast-routing	Enable IP multicast routing.
(config)#exit	Exit Configure mode.

Enabling PIM-SMDM

Enable PIM-SMDM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SMDM on the router.

#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured and Enter interface mode.
(config-if)#ip pim sparse-dense-mode	Enable PIM sparse-dense mode on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured and Enter interface mode.

(config-if)# ip pim sparse-dense-mode	Enable PIM sparse -dense mode on the interface.
(config-if)#exit	Exit interface mode.

Validation

Here is the sample configuration for Router_C:

```
hostname Router_C
!
interface eth0
!
interface eth1
 ip pim sparse-dense-mode
!
interface eth2
 ip pim sparse-dense-mode
!
interface lo
!
!
ip multicast-routing
```

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

```
Router_C#show ip pim interface
```

Address	Interface	VIFindex	Ver/ Mode	Nbr Count
192.168.1.10	eth1	0	v2/SD	0
172.16.1.10	eth2	2	v2/SD	1

Sparse Mode Operation versus Dense Mode Operation

The following examples differentiates the group operating in sparse mode versus dense mode:

- Sparse mode operation when the RP is present for the group
- Dense mode operation when there is no RP for the group

Sparse Mode Operation

Configuring Rendezvous Point Statically for PIM-SMDM

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing

the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in [Figure 9-11](#), 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).

Topology

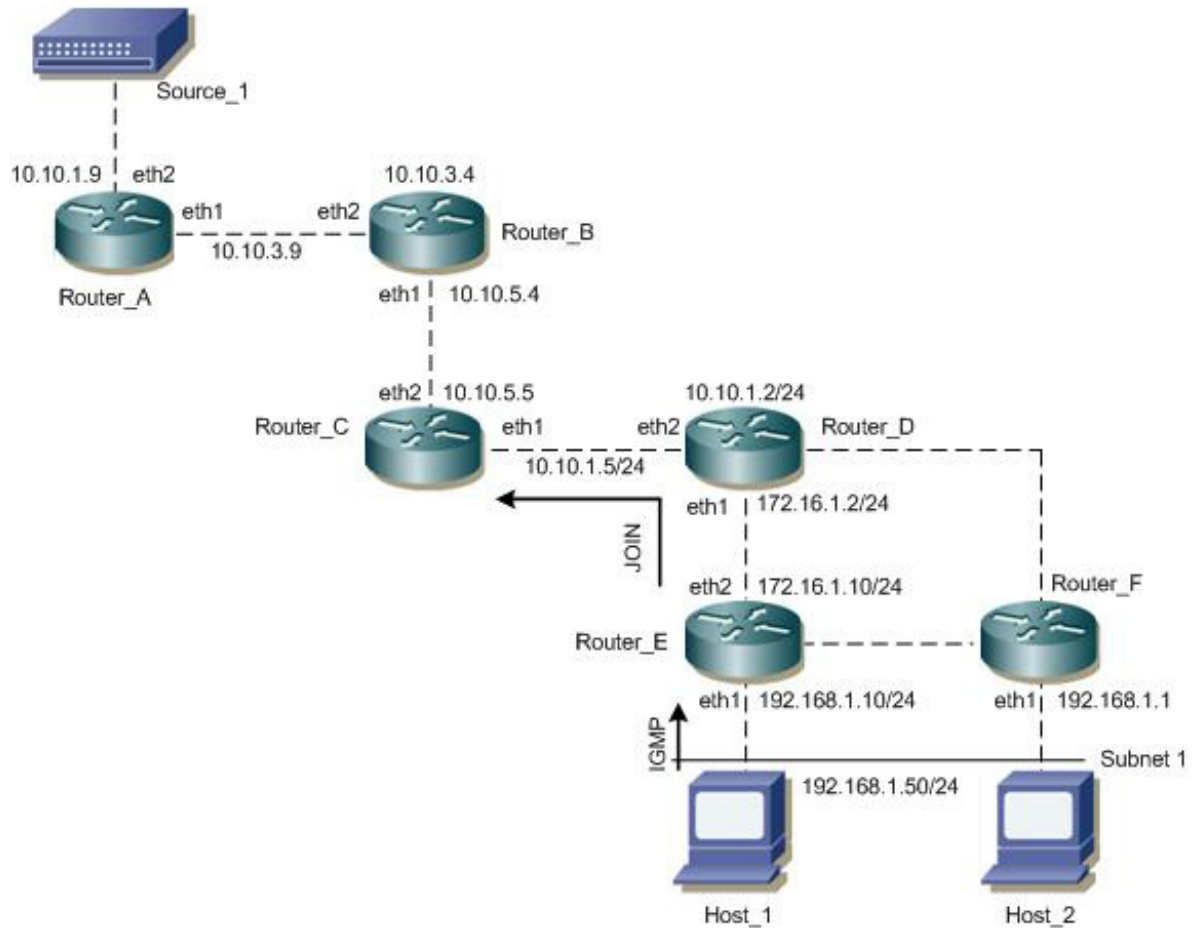


Figure 9-11: PIM-SMDM Configuration Topology (a)

Configure Static RP

#configure terminal	Enter configure mode.
(config)#ip pim rp-address 10.10.1.5	Statically configure an RP address for multicast groups.
(config)#exit	Exit Configure mode.

Validation

Here is the sample configuration for Router_D:

```
hostname Router_D
!
interface eth0
!
interface eth1
 ip pim sparse-dense-mode
!
interface eth2
 ip pim sparse-dense-mode
!
interface lo
!
!
ip multicast-routing
ip pim rp-address 10.10.1.5
!
```

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:

```
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
  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  Count Prior
192.168.1.10     eth1     0      v2/SD  1      1     192.168.1.10
172.16.1.10      eth2     2      v2/SD  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)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
  Local      .....
  Joined    j.....
  Asserted  .....
  Outgoing  o.....
```

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.

```
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)
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  Local      .....
  Joined    j.....
  Asserted  .....
  Outgoing  o.....
```

For configuring Rendezvous point dynamically refer [Configure Rendezvous Point Dynamically Using Bootstrap Router Method](#) and [Configuring Rendezvous Point Statically](#)

Dense-mode Operation

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

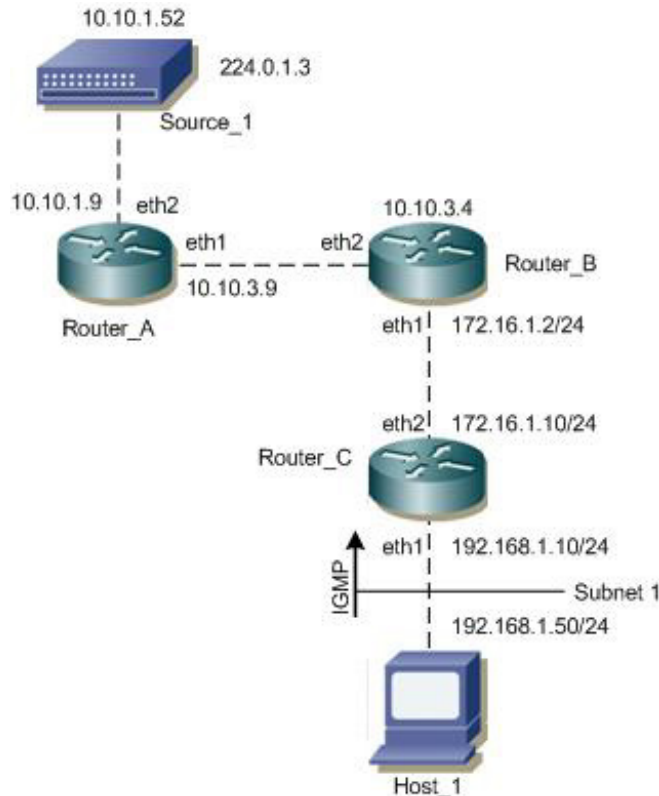


Figure 9-12: PIM-SMDM Configuration Topology (b)

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3

In this example all routers are running PIM-SMDM

1. Host_1 sends an IGMP membership report to Subnet 1
2. After Router_C receives this report, it associates its receiving interface, eth1, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches Router_C, it forwards via the interface, eth1, because there is a local member on this interface for this group. Router_C has a downstream receiver, so it does not send a prune message to its upstream neighbor router, Router_E.

Validation

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

IP Multicast Routing Table

The `show ip pim 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)
```

IP PIM-SMDM Multicast Routing Table

The `show ip pim dense-mode mroute` command 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
```


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`
- `ipv6 mroute`
- `show debugging ip mrib`
- `show ip mroute`
- `show ip mvif`
- `show running-config interface multicast`
- `show running-config interface multicast`

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

<code>all</code>	Enable all IPv4 multicast debugging.
<code>event</code>	Enable debugging of multicast events.
<code>fib-msg</code>	Enable debugging of multicast FIB messages
<code>mrib-msg</code>	Enable debugging of multicast MRIB messages
<code>mrt</code>	Enable debugging of multicast route
<code>mtrace</code>	Enable debugging of multicast traceroute
<code>mtrace-detail</code>	Enable detailed debugging of multicast traceroute messages
<code>nsm-msg</code>	Enable debugging of multicast NSM messages
<code>register-msg</code>	Enable debugging of multicast PIM Register messages
<code>stats</code>	Enable debugging of multicast statistics.
<code>vif</code>	Enable debugging of multicast interface
<code>vrf</code>	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

<code>vrf</code>	Specify the VRF name.
------------------	-----------------------

Default

By default, multicast routing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

ipv6 mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the `no` form of this command to clear a multicast static route.

Command Syntax

```
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X
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 rcv 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 rcv/Reg NACK rcv/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 rcv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent
```

```
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following is a sample output for this command displaying the IP multicast routing table in an abbreviated form:

```
#show ip mroute summary
```

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

```
(10.10.1.52, 224.0.0.13), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

Table 1-3: mroute pointers

Pointers	Description
I	Immediate statistics
T	Timed statistics
F	Forwarder installed
B	Bidirectional
Timers	<ul style="list-style-type: none"> Uptime – route uptime. Statistics Expiry –The time the routing table waits before updating statistics.
Interface State	Interface Time to Live (TTL)

Table 1-4: Show ip mroute output

Entry	Description
(a.d.c.d, 224.x.x.x)	Source Address paired with its Destination Multicast Group Address
uptime	As stated.

Table 1-4: Show ip mroute output

Entry	Description
Owner	The owner is derived from the multicast group notable address (IANA). In the example above, the owner is specified as PIM because it is using the IANA address: 224.0.0.13. Other owners can be OSPF (224.0.0.5), IS-IS (224.0.0.19–21), and so on.
Flags	The flags associated with this mroute table entry.
Incoming interface	The name of the in coming interface (eth1, xe5/2, etc.).
Outgoing interface list	A numbered list of the outgoing interfaces

Table 1-5: 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  Vif  Remote  Uptime
            Idx  Module  Local  Address  Address
wm0          0    PIM-SM  1    192.168.1.53  0.0.0.0  00:04:26
Register    1    PIM-SM  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  Vif  Remote  Uptime
            Idx  Module  Local  Address  Address
wm0          0    PIM-SM  1    192.168.1.53  0.0.0.0  00:05:17
```

Table 1-6: 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 Sparse Mode).

Table 1-6: Show ip mvif output (Continued)

Entries	Description
TTL	Time to Live for the entry.
Local Address	AS stated.
Remote Address	As stated.
Uptime	How long the multicast interface has been operating.

show running-config interface multicast

Use this command to show the running system status and configuration for a multicast interface.

Command Syntax

```
show running-config interface IFNAME ip multicast
```

Parameters

IFNAME Interface name.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#show running-config interface eth1 ip multicast
!
interface eth1
!
```

snmp restart mribd

Use this command to restart SNMP in Multicast Routing Information Base (MRIB)

Command Syntax

```
snmp restart mribd
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal  
(config)#snmp restart mribd
```

CHAPTER 2 L3 IGMP Multicast Commands

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

For IGMP multicast snooping commands, see [Chapter 3, L2 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`

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

<code>all</code>	Debug all IGMP.
<code>decode</code>	Debug IGMP decoding.
<code>encode</code>	Debug IGMP encoding.
<code>events</code>	Debug IGMP events.
<code>fsm</code>	Debug IGMP Finite State Machine (FSM).
<code>tib</code>	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 have no effect on interfaces configured for IGMP proxy.

Use the `no` parameter with this command to return all IGMP related configuration to the default (including IGMP proxy service).

Command Syntax

```
ip igmp
no ip igmp
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp
```

ip igmp access-group

Use this command to control the multicast local-membership groups learned on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP proxy.

Use the `no` parameter with this command to disable this access control.

Command Syntax

```
ip igmp access-group WORD
no ip igmp access-group WORD
```

Parameters

WORD Standard IP access-list name.

Default

No access list configured

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, hosts serviced by Ethernet interface 0 can only join the group 225.2.2.2:

```
#configure terminal
(config)#access-list 1 permit 225.2.2.2 0.0.0.0
(config)#interface eth1
(config-if)#ip igmp access-group xyz
(config-if)#exit
```

ip igmp immediate-leave

In IGMP version 2, use this command to minimize the leave latency of IGMP memberships. This command is used when only one receiver host is connected to each interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP Proxy.

To disable this feature, use the `no` parameter with this command.

Command Syntax

```
ip igmp immediate-leave group-list WORD
no ip igmp immediate-leave
```

Parameters

<code>group-list</code>	Standard access-list name or number that defines multicast groups in which the immediate leave feature is enabled.
<code>WORD</code>	Standard IP access-list name.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one host membership at a time per interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp immediate-leave group-list xyz
(config-if)#exit
(config)#access-list 34 permit 225.192.20.0 0.0.0.255
```

ip igmp join-group

Use this command to configure a join multicast group.

Use the `no` parameter with this command to delete group membership entry.

Command Syntax

```
ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}  
no ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}
```

Parameters

A.B.C.D	Standard IP multicast group address to be configured as a group member.
source	Static source to be joined.
A.B.C.D	Standard IP source address to be configured as a source from where multicast packets originate.

Command Mode

Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

```
#configure terminal  
(config)#interface eth1  
(config-if)#ip igmp join-group 225.1.1.1 source 1.1.1.2  
  
(config-if)#no ip igmp join-group 225.1.1.1 source 1.1.1.2
```

ip igmp last-member-query-count

Use this command to set the last-member query-count value. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax

```
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

Parameter

<2-7> Specify the last member query count value.

Default

The default last member query count value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-count 3
```

ip igmp last-member-query-interval

Use this command to configure the frequency at which the router sends IGMP group-specific host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to set this frequency to the default value.

Command Syntax

```
ip igmp last-member-query-interval <1000-25500>
no ip igmp last-member-query-interval
```

Parameter

<1000-25500> Frequency (in milliseconds) at which IGMP group-specific host query messages are sent.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

The following example changes the IGMP group-specific host query message interval to 2 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-interval 2000
```

ip igmp limit

Use this command to set the maximum number of group membership states, at either the router level or at the interface level. Once the specified number of group memberships is reached, all further local-memberships are ignored. Optionally, an exception access-list can be configured to specify the group-address(es) to be excluded from being subject to the limit.

This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy. The limit applies, individually, to each of its constituent interfaces.

Use the `no` parameter with this command to unset the limit and any specified exception access-list.

Command Syntax

```
ip igmp limit (<1-2097152> (except WORD |)
ip igmp (vrf NAME) limit(<1-2097152> (except WORD |)
no ip igmp limit
no ip igmp (vrf NAME|) limit
```

Parameters

<code>vrf</code>	Specify the VRF name.
<code><1-2097152></code>	Maximum number of group membership states.
<code>except</code>	Number or name that defines multicast groups that are exempted from being subject to configured limit.
<code>WORD</code>	Standard IP access-list name.

Command Mode

Configure mode and Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures an IGMP limit of 100 group-membership states across all interfaces on which IGMP is enabled, and excludes group 224.1.1.1 from this limitation:

```
#configure terminal
(config)#access-list 1 permit 224.1.1.1 0.0.0.0
(config)#ip igmp limit 100 except xyz
```

The following example configures an IGMP limit of 100 group-membership states on eth1:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp limit 100
```

ip igmp mroute-proxy

Use this command to specify the IGMP Proxy service (upstream host-side) interface with which to be associated. IGMP router-side protocol operation is enabled only when the specified upstream proxy-service interface is functional.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the association with the proxy-service interface.

Command Syntax

```
ip igmp mroute-proxy IFNAME
no ip igmp mroute-proxy
```

Parameter

IFNAME	Specify an interface name.
--------	----------------------------

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the eth1 interface as the upstream proxy-service interface for the downstream router-side interface, eth1.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp mroute-proxy eth1
```

ip igmp offlink

Use this command to configure off-link for IGMP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
ip igmp offlink
no ip igmp offlink
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp offlink

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

ip igmp proxy-service

Use this command to designate an interface to be the IGMP proxy-service (upstream host-side) interface, thus enabling IGMP host-side protocol operation on this interface. All associated downstream router-side interfaces will have their memberships consolidated on this interface, according to IGMP host-side functionality.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast-routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the designation of the interface as an upstream proxy-service interface.

Command Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example designates the eth1 interface as the upstream proxy-service interface.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy-service
```

ip igmp proxy unsolicited-report-interval

Use this command to set an unsolicited report interval for an interface designated as an IGMP proxy (upstream host-side).

Use the `no` parameter with this command to remove the unsolicited report interval from the interface.

Command Syntax

```
ip igmp proxy unsolicited-report-interval <1000-25500>
no ip igmp proxy unsolicited-report-interval
```

Parameter

<1000-25500> Specify an unsolicited report interval value in milliseconds.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy unsolicited-report-interval 1234

(config-if)#no ip igmp proxy unsolicited-report-interval
```

ip igmp querier-timeout

Use this command to set the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To restore the default value, use the `no` parameter with this command.

Command Syntax

```
ip igmp querier-timeout <60-300>
no ip igmp querier-timeout
```

Parameter

<60-300>	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier.
----------	--

Default

255 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp querier-timeout 120
```

ip igmp query-interval

Use this command to set the frequency of sending IGMP host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default frequency, use the `no` parameter with this command.

Note: Querier timeout changes by changing query interval.

Command Syntax

```
ip igmp query-interval <1-18000>
no ip igmp query-interval
```

Parameter

<1-18000> Frequency (in seconds) at which IGMP host query messages are sent.

Default

Default query interval is 125 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example changes the frequency of sending IGMP host-query messages to 2 minutes:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-interval 120
```

ip igmp query-max-response-time

Use this command to set the maximum response time advertised in IGMP queries. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
ip igmp query-max-response-time <1-240>
no ip igmp query-max-response-time
```

Parameter

<1-240> Maximum response time (in seconds) advertised in IGMP queries.

Default

10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-max-response-time 8
```

ip igmp ra-option

Use this command to configure strict RA (Router Advertisement) validation for IGMP.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
ip igmp ra-option
no ip igmp ra-option
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp ra-option

(config-if)#no ip igmp ra-option
```

ip igmp robustness-variable

Use this command to set the robustness variable value on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default value on an interface, use the `no` parameter with this command.

Command Syntax

```
ip igmp robustness-variable <2-7>
no ip igmp robustness-variable
```

Parameter

<2-7> Specify the robustness variable value.

Default

Default robustness variable value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp robustness-variable 3
```

ip igmp ssm-map enable

Use this command to enable SSM mapping on the router. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to disable SSM mapping.

Command Syntax

```
ip igmp ssm-map enable
ip igmp (vrf NAME|) ssm-map enable
no ip igmp ssm-map enable
no ip igmp (vrf NAME|) ssm-map enable
```

Parameter

<code>vrf</code>	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

<code>vrf</code>	Specify the VRF name.
<code>WORD</code>	Standard IP access-list name.
<code>A.B.C.D</code>	Source address to use for static map group.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to configure an SSM static mapping for group-address 224.1.1.1

Note: `access-list` can only be a `permit` type `access-list`

```
#configure terminal
(config)# ip igmp ssm-map static xyz 1.2.3.4
(config)# access-list 1 permit 224.1.1.1 0.0.0.255
```

ip igmp static-group

Use this command to statically configure group membership entries on an interface. To statically add only a group membership, do not specify any parameters. This command applies to IGMP operation on a specific interface to statically add group and/or source records; on a VLAN interface to statically add group and/or source records.

Use the `no` parameter with this command to delete static group membership entries.

Command Syntax

```
ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)
no ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)
```

Parameters

A.B.C.D	Standard IP Multicast group address to be configured as a static group member.
source	Static source to be joined.
A.B.C.D	Standard IP source address to be configured as a static source from where multicast packets originate.
ssm-map	Mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate these (*, G) groups' memberships to (S, G) memberships for use with PIM-SSM.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show how to statically add group and/or source records for IGMP:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.3

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.4 source 1.2.3.4

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.5 source ssm-map
```

ip igmp startup-query-count

Use this command to set a startup query count for IGMP.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ip igmp startup-query-count <2-10>
no ip igmp startup-query-count
```

Parameters

<2-10> Specify a startup query count value.

Default

The default value 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-count 2

(config-if)#no ip igmp startup-query-count
```

ip igmp startup-query-interval

Use this command to set a query interval value for IGMP.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ip igmp startup-query-interval <1-18000>
no ip igmp startup-query-interval
```

Parameters

<1-18000> Specify a startup query interval value in seconds.

Default

The default value 31 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-interval 1

(config-if)#no ip igmp startup-query-interval
```

ip igmp version

Use this command to set the current IGMP protocol version on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ip igmp version <1-3>
no ip igmp version
```

Parameters

<1-3> Specify IGMP protocol version number.

Default

The default IGMP protocol version number is 3.

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp version 2
```

show debugging ip igmp

Use this command to display the status of the debugging of the IGMP system, or a specific VRF in the IGMP system.

Command Syntax

```
show debugging ip igmp
show debugging ip igmp (vrf NAME|)
```

Parameters

`vrf` Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

```
#show debugging ip igmp
IGMP Debugging status:
IGMP Decoder debugging is on
IGMP Encoder debugging is on
IGMP Events debugging is on
IGMP FSM debugging is on
IGMP Tree-Info-Base (TIB) debugging is on
```

show ip igmp groups

Use this command to display the multicast groups with receivers connected to the router and learned through IGMP.

Command Syntax

```
show ip igmp groups (detail|)
show ip igmp groups A.B.C.D (detail|)
show ip igmp groups IFNAME (detail|)
show ip igmp groups IFNAME A.B.C.D (detail|)
show ip igmp (vrf NAME|) groups (detail|)
show ip igmp (vrf NAME|) groups A.B.C.D (detail|)
show ip igmp (vrf NAME|) groups IFNAME (detail|)
show ip igmp (vrf NAME|) groups IFNAME A.B.C.D (detail|)
```

Parameters

vrf	Specify the VRF name.
A.B.C.D	Address of multicast group.
IFNAME	Name of the interface.
detail	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following command displays local-membership information for all interfaces:

```
rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
SG - Static Group, SS - Static Source)
Interface:      eth1
Group:          224.1.1.1
Flags:          L
Uptime:         00:00:04
Group mode:     Exclude (Expires: 00:04:15, Static)
Last reporter:  3.3.3.3
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)
Include Source List :
Source Address Uptime      v3 Exp      Fwd Flags
2.2.2.2         00:00:04  stopped   Yes L
```

[Table 2-7](#) shows the flags codes displayed at the start of a group entry.

Table 2-7: Flags

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

[Table 2-8](#) explains the output fields.

Table 2-8: show ip igmp groups output

Entry	Description
Interface	The interface on which multicast is operating.
Group	The Multicast group, identified by a multicast IP address.
Flags	Flag on this interface – in this case, the flag indicates that the multicast is Local. See Table 2-7 .
Uptime	The amount of time that the multicast connection has been up.
Group mode	The group mode is determined by interactions between IGMP router database entries, which is beyond the scope of this document. For a detailed description of these interactions, see RFC 3376.
Last reporter	The IPv4 address of the last host to send multicast information.
Group source list	A list of flags that indicate the state of the multicast connections. See Table 2-7 .
Include Source List	A table containing parameters about the multicast session: <ul style="list-style-type: none"> • Source Address – The IP address of the Source(s) connected to the multicast hosts. • Uptime – The multicast session's uptime. • v3 Exp – Tells whether IGMPv3 Explicit Tracking is running or not. • Fwd – Whether IGMP information is being forwarded by this device. • Flags – See Table 2-7.

show ip igmp interface

Use this command to display the state of IGMP, IGMP Proxy service for a specified interface, or all interfaces.

Command Syntax

```
show ip igmp interface (IFNAME|)
show ip igmp (vrf NAME|) interface (IFNAME|)
```

Parameters

vrf	Specify the VRF name.
interface	Specify the interface parameter.
IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the IGMP interface status on all interfaces enabled for IGMP.

```
#show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds|
#
```

[Table 2-9](#) explains the output fields.

Table 2-9: show ip igmp interface

Entry	Description
Interface	Interface type and number
IGMP Active	IGMP status – whether Active or Inactive; whether this interface is a querier; IGMP version (v1, v2, or v3).
IGMP querying router	IP address of the designated router for this LAN segment.
IGMP query interval	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages.
IGMP querier timeout	An interval of time that the software uses when deciding to take over as the querier.

Table 2-9: show ip igmp interface (Continued)

Entry	Description
IGMP max query response time	An interval of time that is advertised as the maximum response time that is advertised in IGMP queries.
Last member query response interval	This interval is the maximum amount of time between query messages that the querier will wait before sending messages that indicate that the multicast session has ended.
Group Membership interval	A group membership interval timer is maintained for each dynamic multicast group added to a downstream interface in the table. The timer is refreshed when a membership report for a multicast group is received. If the timer expires, the multicast group is removed from the table.

show ip igmp proxy

Use this command to display the state of IGMP Proxy services for a specified interface or for all interfaces.

Command Syntax

```
show ip igmp proxy groups (detail|)
show ip igmp proxy groups A.B.C.D (detail|)
show ip igmp proxy groups IFNAME (detail|)
show ip igmp proxy groups IFNAME A.B.C.D (detail|)
show ip igmp (vrf NAME|) proxy groups (detail|)
show ip igmp (vrf NAME|) proxy groups A.B.C.D (detail|)
show ip igmp (vrf NAME|) proxy groups IFNAME (detail|)
show ip igmp (vrf NAME|) proxy groups IFNAME A.B.C.D (detail|)
```

Parameters

vrf	Specify the VRF name.
groups	IGMP proxy group membership information.
A.B.C.D	Address of multicast group.
IFNAME	The name of the VLAN interface.
detail	IGMPv3 source information

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1

#show ip igmp proxy groups

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


Table 2-10 explains the output fields.

Table 2-10: show ip igmp proxy output

Entry	Description
Interface	Interface and Index of the interface.
Administrative status	Depends on the interface states – Enabled only if both host and downstream interfaces are up. Otherwise, Disabled if only one interface is up.
Operational status	Depends on Administrative status – either Up or Down depending on Administrative status of corresponding interfaces.
Upstream interface	As stated.
Number of multicast groups	The number of multicast groups supported by this proxy.

Table 2-11 explains the output fields.

Table 2-11: show ip igmp proxy groups output

Entry	Description
Group Address	Multicast address associated with each group.
Interface	Interface name, such as eth1, xe3/1, etc..
State	The state of the proxy group – can be either Active or Inactive.
Member state	The state of the proxy group member – can be either Idle or Delay, Idle is the default state.

show ip igmp ssm-map

Use this command to display IGMP SSM-map data.

Command Syntax

```
show ip igmp ssm-map
show ip igmp ssm-map A.B.C.D
show ip igmp (vrf NAME|) ssm-map
show ip igmp (vrf NAME|) ssm-map A.B.C.D
```

Parameters

vrf	Specify the VRF name.
A.B.C.D	Address of multicast group.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ip igmp ssm-map
SSM Mapping : Enabled
Database    : Static mappings configured
```

show running-config interface igmp

Use this command to show the running system status and configuration for IGMP.

Command Syntax

```
show running-config interface IFNAME ip igmp
```

Parameters

IFNAME Interface name.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
!
```


CHAPTER 3 L2 IGMP Snooping Multicast Commands

This chapter describes commands for Internet Group Management Protocol (IGMP) multicast 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](#)

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
```

igmp snooping fast-leave

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

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

Command Syntax

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

Parameters

None

Default

IGMP Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

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

igmp snooping mrouter

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

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

Command Syntax

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

Parameter

IFNAME Specify the name of the interface.

Default

IGMP Snooping mrouter processing is disabled.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

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

igmp snooping querier

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

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

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

Command Syntax

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

Default

By default, Querier is disabled

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

igmp snooping report-suppression

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

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

Command Syntax

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

Default

By default, report suppression is enabled.

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

Applicability

This command was introduced before OcnOS version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#sh igmp snooping interface
Global IGMP Snooping information
IGMP Snooping Enabled
IGMPv1/v2 Report suppression Enabled
IGMPv3 Report suppression Enabled

IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
  xe5/1

IGMP Snooping information for vlan1.2
IGMP Snooping enabled
Snooping Querier enabled, address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds
```

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

show igmp snooping groups

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

Command Syntax

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

Parameters

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

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

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

#show igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

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

#show igmp snooping groups 230.0.0.1
```

```

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

#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
V3
200    230.0.0.1                xe1        S      00:02:47  static  0.0.0.0

#show igmp snooping groups vlan1.200 detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

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

```

Table 3-12: Show igmp snooping groups

Entries	Description
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Group	The multicast group identified by an IPv4 address.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.
Group mode	As stated.

Table 3-12: Show igmp snooping groups (Continued)

Entries	Description
Last reporter	<p>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.</p> <p>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.</p>
Vlan	VLAN number ID.
Group/Source Address	Multicast group and source addresses.
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.
Expires	Either by a timeout (IGMPv1) or by checking whether the member is still a part of the multicast (IGMPv2 or v3). Can also be statically configured.
Last Reporter	Indicates that the host wants to join a particular multicast group.
Version	IGMP version (v1, v2, or v3).

show igmp snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax

```
show igmp snooping mrouter IFNAME
```

Parameters

IFNAME Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#show igmp snooping mrouter vlan1.1
VLAN    Interface                      IP-address    Expires
1        xe1(static)
```

show igmp snooping statistics

Use this command to display IGMP Snooping statistics data.

Command Syntax

```
show igmp snooping statistics interface IFNAME
```

Parameters

IFNAME Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show igmp snooping statistics interface vlan1.1
IGMP Snooping statistics for vlan1.1
Group Count          : 1
IGMPv1 reports received : 0
IGMPv2 reports received : 0
IGMPv2 leaves received  : 0
IGMPv3 reports received : 0
IGMPv1 query warnings  : 0
IGMPv2 query warnings  : 0
IGMPv3 query warnings  : 0
```

CHAPTER 4 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`
- `ip 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 cisco-register-checksum`
- `ip pim crp-cisco-prefix`
- `ip pim dr-priority`
- `ip pim ecmp-bundle`
- `ip pim exclude-genid`

- `ip pim hello-holdtime`
- `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 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`

clear ip mroute

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

Command Syntax

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

Parameters

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

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

clear ip msdp peer

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

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

Command Syntax

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

Parameters

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

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

clear ip msdp sa-cache

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

Command Syntax

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

Parameters

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

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

clear ip pim sparse-mode

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

Command Syntax

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

Parameters

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

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

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

debug ip pim

Use this command to enable debugging for PIM.

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

Command Syntax

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

Parameters

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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>in</code>	Debug incoming packets
<code>out</code>	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 is introduced in OcnOS version 5.1

Examples

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

Parameters

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>at</code>	Use this option to turn on or off debugging of the PIM Assert Timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

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

debug ip pim timer bsr

Use this command to enable debugging of PIM BSR time.

Use the `no` option with this command to disable debugging of the PIM BSR timer.

Command Syntax

```
debug ip pim timer bsr
debug ip pim timer bsr bst
debug ip pim timer bsr crp
debug ip pim (vrf NAME|) timer bsr
debug ip pim (vrf NAME|) timer bsr bst
debug ip pim (vrf NAME|) timer bsr crp
no debug ip pim timer bsr
no debug ip pim timer bsr bst
no debug ip pim timer bsr crp
no debug ip pim (vrf NAME|) timer bsr
no debug ip pim (vrf NAME|) timer bsr bst
no debug ip pim (vrf NAME|) timer bsr crp
```

Parameters

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>bst</code>	Turn on or turn off the bootstrap debugging timer
<code>crp</code>	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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>ht</code>	Turn on or turn off the PIM Hello debugging timer (ht)
<code>nlt</code>	Turn on or turn off the PIM Neighbor Liveliness debugging timer (nlt)
<code>tht</code>	Turn on or turn off the Triggered Hello Timer (tht)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#configure terminal
```

```
(config)#debug ip pim timer hello ht
```

debug ip pim timer joinprune

Use this command to enable debugging of various PIM JoinPrune timers.

Use the no option with this command to disable the debugging of the PIM JoinPrune timers.

Command Syntax

```
debug ip pim timer joinprune
debug ip pim timer joinprune et
debug ip pim timer joinprune kat
debug ip pim timer joinprune jt
debug ip pim timer joinprune ot
debug ip pim timer joinprune ppt
debug ip pim (vrf NAME|) timer joinprune
debug ip pim (vrf NAME|) timer joinprune et
debug ip pim (vrf NAME|) timer joinprune kat
debug ip pim (vrf NAME|) timer joinprune jt
debug ip pim (vrf NAME|) timer joinprune ot
debug ip pim (vrf NAME|) timer joinprune ppt
no debug ip pim timer joinprune
no debug ip pim timer joinprune et
no debug ip pim timer joinprune kat
no debug ip pim timer joinprune jt
no debug ip pim timer joinprune ot
no debug ip pim timer joinprune ppt
no debug ip pim (vrf NAME|) timer joinprune
no debug ip pim (vrf NAME|) timer joinprune et
no debug ip pim (vrf NAME|) timer joinprune kat
no debug ip pim (vrf NAME|) timer joinprune jt
no debug ip pim (vrf NAME|) timer joinprune ot
no debug ip pim (vrf NAME|) timer joinprune ppt
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
et	Turn on or turn off the PIM JoinPrune expiry timer (et)
jt	Turn on or turn off the PIM JoinPrune upstream Join Timer (jt)
kat	Turn on or turn off the PIM JoinPrune Keep Alive timer (kat)
ot	Turn on or turn off the PIM JoinPrune Upstream Override Timer (ot)
ppt	Turn on or turn off the PIM JoinPrune PrunePending Timer ((ppt)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer joinprune et
```

debug ip pim timer register

Use this command to enable the PIM register timer's debugging.

Use the no option with this command to disable the PIM register timer's debugging.

Command Syntax

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

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
rst	Turn on or turn off the PIM Register Stop Timer (rst)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

```
#debug ip pim timer register
```

ip msdp default-peer

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

You can have multiple active default peers:

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

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

Command Syntax

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

Parameters

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

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

ip msdp mesh-group

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

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

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

Command Syntax

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

Parameters

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

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

ip msdp originator-id

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

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

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

Command Syntax

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

Parameters

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

Default

The RP address is used as the originator ID.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

ip msdp password

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

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

Command Syntax

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

Parameters

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

Default

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

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

ip msdp peer

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

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

Command Syntax

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

Parameters

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

Default

By default, all `ip msdp` options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

ip 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-SP 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

<code>dense-mode</code>	Enable PIM dense-mode operation
<code>sparse-mode</code>	Enable PIM sparse-mode

Default

By default, the `ip pim` option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode

(config)#interface eth0
(config-if)#no ip pim dense-mode

(config)#interface eth0
(config-if)#ip pim sparse-mode
(config-if)#no ip pim sparse-mode
```

ip pim accept-register

Use this command to configure the ability to filter out multicast sources specified by the given access-list at the RP, so that the RP will accept/refuse to perform the Register mechanism for the packets sent by the specified sources. By default, the RP accepts Register packets from all multicast sources.

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

Command Syntax

```
ip pim accept-register list WORD
ip pim (vrf NAME|) accept-register list WORD
no ip pim accept-register
no ip pim (vrf NAME|) accept-register
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
WORD	Name of a standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim accept-register list xyz

(config)#no ip pim accept-register
```

ip pim anycast-rp

Use this command to configure the Anycast RP in the RP set.

Use the no option with this command to remove the configuration.

Command Syntax

```
ip pim anycast-rp A.B.C.D A.B.C.D
ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D
no ip pim anycast-rp A.B.C.D
no ip pim anycast-rp A.B.C.D A.B.C.D
no ip pim (vrf NAME|) anycast-rp A.B.C.D
no ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D
```

Parameters

vrf	The VPN routing/forwarding instance.
NAME	Specify the name of the VPN routing/forwarding instance.
A.B.C.D	Unicast IP address of the Anycast RP set. An Anycast RP set is a collection of RPs in the same domain.
A.B.C.D	Destination IP address where Register messages are copied and sent. A Member RP is an individual RP member in the Anycast RP set.

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to configure the Anycast RP in the RP set.

```
#configure terminal
(config)#ip pim anycast-rp 1.1.1.1 10.10.10.10
```

The following example shows how to remove the configuration.

```
#configure terminal
(config)#no ip pim anycast-rp 1.1.1.1 10.10.10.10
```

ip pim 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

<code>disable</code>	Useful when PIMv4 BFD is enabled at global level (refer command <code>ip pim bfd all-interfaces</code>) and it is required to disable <code>pim bfd</code> 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-SP 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

<code>vrf</code>	The VPN routing/forwarding instance.
<code>NAME</code>	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-DC 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-SP 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-SP 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-SP 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-SP 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 Bundles.

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

Configure mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3

Examples

```
OcNOS(config)#ip pim bind ecmp-bundle ebundl
OcNOS(config)#commit
OcNOS(config)#no ip pim bind ecmp-bundle
OcNOS(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 eth0
(config-if)#ip pim bsr-border

(config)#interface eth0
(config-if)#no ip pim bsr-border
```

ip pim bsr-candidate

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

Use the `no` option with this command to disable this function.

Command Syntax

```
ip pim (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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>IFNAME</code>	Specify the name of the interface
<code><0-32></code>	Specify a hash mask length for RP selection
<code><0-255></code>	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

```
(config)#ip pim bsr-candidate eth0 20 30
(config)#ip pim bsr-candidate eth1
(config)#no ip pim bsr-candidate
```

ip pim cisco-register-checksum

Use this command to configure the option to calculate the register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

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

Command Syntax

```
ip pim cisco-register-checksum
ip pim cisco-register-checksum group-list WORD
ip pim (vrf NAME|) cisco-register-checksum
ip pim (vrf NAME|) cisco-register-checksum group-list WORD
no ip pim cisco-register-checksum
no ip pim cisco-register-checksum group-list WORD
no ip pim (vrf NAME|) cisco-register-checksum
no ip pim (vrf NAME|) cisco-register-checksum group-list WORD
```

Parameters

vrf	The VPN routing/forwarding instance.
NAME	Specify the name of the VPN routing/forwarding instance.
group-list	Use this parameter to configure the option to calculate the register checksum over the whole packet on multicast groups specified by the access-list.
WORD	IP named standard access list.

Default

This command is disabled by default. By default, Register Checksum is calculated only over the header.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim cisco-register-checksum

#configure terminal
(config)#ip pim cisco-register-checksum group-list xyz
(config)#ip access-list 34 permit 224.0.1.3
```

ip pim 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 (vrf NAME|) crp-cisco-prefix
no ip pim (vrf NAME|) 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 eth0
(config-if)#ip pim dr-priority 11234

(config)#interface eth0
(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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>WORD</code>	ECMP bundle name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

```
OcnOS(config)#ip pim ecmp-bundle ebund1
OcnOS(config)#commit
OcnOS(config)#no ip pim ecmp-bundle ebund1
OcnOS(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 eth0
(config-if)#ip pim exclude-genid

(config)#interface eth0
(config-if)#no ip pim exclude-genid
```

ip pim hello-holdtime

Use this command to configure a hello holdtime other than the default ($3.5 * \text{hello_interval}$ 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 ($3.5 * \text{current hello_interval}$) 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 ($3.5 * \text{hello_interval}$). Otherwise, the configured value is maintained.

Use the `no` option with this command to remove the configured hello-holdtime.

Command Syntax

```
ip pim hello-holdtime <1-65535>
no ip pim hello-holdtime
```

Parameter

<1-65535> Range of values for hello-holdtime, in seconds

Default

The default hello-holdtime is 105 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-holdtime 123

(config)#interface eth0
(config-if)#no ip pim hello-holdtime
```

ip pim hello-interval

Use this command to configure a hello interval value other than the default. When a hello-interval is configured and hello-holdtime is not configured, or when the hello-holdtime value configured is less than the new hello-interval value, the holdtime value is modified to (3.5 * hello_interval). Otherwise, the hello-holdtime value is the configured value.

Use the `no` option with this command to reset the hello-interval to its default value.

Command Syntax

```
ip pim hello-interval <1-18724>
no ip pim hello-interval
```

Parameter

<1-18724> Range of values for the hello-interval. No fractional values are allowed in seconds.

Default

The default value for hello-interval is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-interval 123

(config)#interface eth0
(config-if)#no ip pim hello-interval
```

ip pim ignore-rp-set-priority

Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to remove this setting.

Command Syntax

```
ip pim ignore-rp-set-priority
ip pim (vrf NAME|) ignore-rp-set-priority
no ip pim ignore-rp-set-priority
no ip pim (vrf NAME|) ignore-rp-set-priority
```

Parameters

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code><1-65535></code>	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

```
OcNOS#configure terminal
OcNOS(config)#interface eth0
OcNOS(config-if)#ip pim neighbor-filter xyz
OcNOS(config-if)#commit
OcNOS(config-if)#no ip neighbor-filter
OcNOS(config-if)#commit
OcNOS(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

<code>dense-mode</code>	Enable passive operation for PIM dense-mode
<code>sparse-mode</code>	Enable passive operation for PIM sparse-mode

Default

By default, the `ip pim` option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode passive

(config)#interface eth0
(config-if)#no ip pim dense-mode passive

#configure terminal
(config)#interface eth0
(config-if)#ip pim sparse-mode passive

(config)#interface eth0
(config-if)#no ip pim sparse-mode passive
```

ip pim propagation-delay

Use this command to configure a propagation delay value for PIM.

Use the no option with this command to return the propagation delay to its default value.

Command Syntax

```
ip pim propagation-delay <0-32767>
no ip pim propagation-delay
```

Parameter

<0-32767> Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 1000 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim propagation-delay 1000

(config)#interface eth0
(config-if)#no ip pim propagation-delay
```

ip pim 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-SP 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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>A.B.C.D</code>	The IP address to use as the source of the register packets
<code>IFNAME</code>	The name of the interface to use as the source of the register packets

Default

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-source 3.3.3.2
OcNOS(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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>A.B.C.D</code>	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 Bootstrap 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

<code>bidir</code>	Bidirectional RP address
<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>WORD</code>	Standard Access-list name
<code>override</code>	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>|)
no ip pim rp-candidate (IFNAME|)
no ip pim (vrf NAME) rp-candidate (IFNAME|)
```

Parameters

vrf NAME	The VPN routing/forwarding instance
IFNAME	Specify an interface name
WORD	A named standard access list
group-list	Group Ranges for this C-RP
interval	C-RP advertisement interval
priority	Candidate-RP priority
<0-16383>	Range of values for candidate-RP advertisement interval, in seconds
<0-255>	Range of values for priority of an RP candidate

Default

The ip pim rp-candidate default priority is 192 and interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim rp-candidate eth0

(config)#no ip pim rp-candidate eth0
```

ip pim rp-register-kat

Use this command to configure a Keepalive Timer (KAT) value for (S,G) states at RP to monitor PIM register packets, overriding the generic KAT timer value.

Use the no option to remove this configuration.

Command Syntax

```
ip pim rp-register-kat <1-65535>
ip pim (vrf NAME|) rp-register-kat <1-65535>
no ip pim rp-register-kat
no ip pim (vrf NAME|) rp-register-kat
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for a KAT time in seconds

Default

The ip pim rp-register-kat default is 60 seconds.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim rp-register-kat 3454

(config)#no ip pim rp-register-kat
```

ip pim spt-threshold

Use this command to turn on the ability of the last-hop PIM router to switch to SPT.

Use the `no` option with this command to turn off the ability of the last-hop PIM router to switch to SPT.

Note: This option is binary, meaning that the switching to SPT happens either at the receiving of the first data packet or not at all. It is not rate-based.

Command Syntax

```
ip pim spt-threshold
ip pim spt-threshold group-list WORD
ip pim (vrf NAME|) spt-threshold
ip pim (vrf NAME|) spt-threshold group-list WORD
no ip pim spt-threshold
no ip pim spt-threshold group-list WORD
no ip pim (vrf NAME|) spt-threshold
no ip pim (vrf NAME|) spt-threshold group-list WORD
```

Parameters

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>group-list</code>	Enable the ability for the last-hop PIM router to switch to SPT for multicast group addresses indicated by the given access-list
<code>WORD</code>	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

<code>vrf</code>	The VPN routing/forwarding instance
<code>NAME</code>	Specify the name of the VPN routing/forwarding instance
<code>default</code>	This keyword defines the 232/8 group range for SSM
<code>range</code>	Define an access-list for group range to use for SSM
<code>WORD</code>	A named standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcnOS version 1.3.

Example

The following example shows how to configure SSM service for the IP address range defined by access list 10:

```
#configure terminal
(config)#access-list 10 permit 225.1.1.1
(config)#ip pim ssm range xyz
```

ip pim state-refresh origination-interval

Use this command to configure a PIM-DM State-Refresh origination interval other than the default value. The origination interval is the number of seconds between PIM-DM State Refresh control messages.

Use the `no` option with this command to return the origination interval to its default value.

Command Syntax

```
ip pim state-refresh origination-interval <1-100>
no ip pim state-refresh origination-interval
```

Parameter

<1-100> Range of values for state-refresh origination interval, in seconds

Note: No fractional values are allowed for the interval time.

Default

The default state-refresh origination interval is 60 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim state-refresh origination-interval 65

(config)#interface eth0
(config-if)#no ip pim state-refresh origination-interval
```

ip pim unicast-bsm

Use this command to enable support for sending and receiving unicast Bootstrap Messages (BSM) on an interface. This command supports backward-compatibility with older versions of the Bootstrap Router specification, which specifies unicast BSM to refresh the state of new or restarting neighbors.

Use the `no` option with this command to disable unicast bootstrap messaging on an interface.

Command Syntax

```
ip pim unicast-bsm
no ip pim unicast-bsm
```

Parameters

None

Default

Unicast bootstrap messaging is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim unicast-bsm

(config)#interface eth0
(config-if)#no ip pim unicast-bsm
```

show debugging ip pim

Use this command to display the debug status for the PIM process.

Command Syntax

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

Parameters

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

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcnOS version 1.3.

Examples

```
#show debugging ip pim
PIM Debugging status:
PIM event debugging is on
PIM MFC debugging is on
PIM state debugging is on
PIM incoming packet debugging is on
PIM outgoing packet debugging is on
PIM Hello HT timer debugging is on
PIM Hello NLT timer debugging is on
PIM Hello THT timer debugging is on
PIM Join/Prune JT timer debugging is on
PIM Join/Prune ET timer debugging is on
PIM Join/Prune PPT timer debugging is on
PIM Join/Prune KAT timer debugging is on
PIM Join/Prune OT timer debugging is on
PIM Assert AT timer debugging is on
PIM Register RST timer debugging is on
PIM Bootstrap BST timer debugging is on
PIM Bootstrap CRP timer debugging is on
PIM mib debugging is on
PIM nexthop debugging is on
PIM mtrace debugging is on
PIM NSM debugging is on
PIM MSDP debugging is on
```

show debugging pim

Use this command to display the status of debugging for PIM.

Command Syntax

```
show debugging pim
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This command displays one of several status:

```
#show debugging pim
PIM Debugging status:
PIM event debugging is on
PIM MFC debugging is on
PIM state debugging is on
PIM incoming packet debugging is on
PIM outgoing packet debugging is on
PIM Hello HT timer debugging is on
PIM Hello NLT timer debugging is on
PIM Hello THT timer debugging is on
PIM Join/Prune JT timer debugging is on
PIM Join/Prune ET timer debugging is on
PIM Join/Prune PPT timer debugging is on
PIM Join/Prune KAT timer debugging is on
PIM Join/Prune OT timer debugging is on
PIM Assert AT timer debugging is on
PIM Register RST timer debugging is on
PIM Bootstrap BST timer debugging is on
PIM Bootstrap CRP timer debugging is on
PIM mib debugging is on
PIM nexthop debugging is on
PIM mtrace debugging is on
PIM NSM debugging is on
PIM MSDP debugging is on
```

show ip msdp peer

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

Command Syntax

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

Parameters

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

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ip msdp peer

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

Table 4-13: show ip msdp peer output

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

show ip msdp sa-cache

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

You can specify zero, one, or two addresses:

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

Command Syntax

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

Parameters

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

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

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

Table 4-14: show ip msdp sa-cache output

Entry	Description
MSDP Source-Active Cache	<ul style="list-style-type: none">• (S,G) address pair – Source address, multicast address• RP – Reverse Path address• RRF-Peer – Reverse Path Forwarding address• Uptime – as stated• Exptime – Time until entry timeout

show ip pim interface

Use this command to display PIM interface information.

Command Syntax

```
show ip pim interface
show ip pim interface detail
show ip pim (vrf NAME|) interface
show ip pim (vrf NAME|) interface detail
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
detail	Display detailed information about a PIM interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

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

The output for PIM ECMP Redirect is as below:

```
rtr6#show ip pim interface detail
eth1 (vif 0):
  Address 192.168.10.57, DR 192.168.10.57
  Hello period 30 seconds, Next Hello in 18 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.57 Local-ID 3
  Neighbors:
    192.168.10.52

eth2 (vif 2):
  Address 192.168.1.57, DR 192.168.1.152
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.57 Local-ID 4
  ECMP REDIRECT, bundle : ecmpbundle, status : allowed
  Neighbors:
```

```
192.168.1.149
192.168.1.150
192.168.1.152
```

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 4-15: 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-SP version 4.0.

Examples

```
Router# show ip pim interface df
```

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

```
Router# show ip pim interface eth1 df 10.10.0.3
```

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

show ip pim mroute

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

Command Syntax

```
show ip pim mroute (detail|)
show ip pim mroute A.B.C.D (detail|)
show ip pim mroute A.B.C.D A.B.C.D (detail|)
show ip pim (vrf NAME|) mroute (detail|)
show ip pim (vrf NAME|) mroute A.B.C.D (detail|)
show ip pim (vrf NAME|) mroute A.B.C.D A.B.C.D (detail|)
```

Parameter

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

Note: A group IP address and a source IP address cannot be simultaneously

detail	Display detailed PIM multicast routing table information
--------	--

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim mroute

IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
Local      .....
Joined    j.....
Asserted  .....
Outgoing  o.....
```


Table 4-16: 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
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 4-17: 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 4-17: Show ip pim neighbor output

Entry	Description
Lan delay:	<p>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:</p> <p>neighbor.lan_prune_delay_present A flag indicating if the LAN Prune Delay option was present in the Hello message.</p> <p>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.</p> <p>neighbor.propagation_delay The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message.</p> <p>neighbor.override_interval The Override_Interval field of the LAN Prune Delay option (if present) in the Hello message.</p> <p>The additional state described above is deleted along with the DR neighbor state when the neighbor timeout expires.</p>
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 4-18: 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 4-18: Show ip pim bsr-router output (Continued)

Entry	Description
Role	Specifies whether the BSR is the Candidate BSR or a Non-candidate BSR
State	<ul style="list-style-type: none"><li data-bbox="564 373 1453 436">• The current state of a Candidate BSR, one of the following: Candidate-BSR, Pending-BSR, or Elected-BSR.<li data-bbox="564 449 1501 512">• 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 4-19: 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 4-20: 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 4-21: 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
```


Index

B

begin modifier 16
 BGP community value
 command syntax 14
 Bootstrap Router 44
 bootstrap router 246
 braces
 command syntax 13
 BSR 44, 246
 BSR validation 53

C

clear ip igmp 122
 clear ip mroute 106, 173
 clear ip msdp sa-cache 176
 clear ip pim sparse-mode bsr 177
 command abbreviations 12
 command completion 12
 command line
 errors 12
 help 11
 keyboard operations 15
 command modes 19
 configure 19
 exec 19
 interface 19
 privileged exec 19
 router 19
 command negation 13
 command syntax
 ? 14
 . 14
 () 13
 {} 13
 | 13
 A.B.C.D/M 14
 AA:NN 14
 BGP community value 14
 braces 13
 conventions 13
 curly brackets 13
 HH:MM:SS 14
 IFNAME 14
 interface name 14
 IPv4 address 14
 IPv6 address 14
 LINE 14
 lowercase 13
 MAC address 14
 monospaced font 13
 numeric range 14
 parantheses 13
 parentheses 13

period 14
 question mark 14
 square brackets 14
 time 14
 uppercase 13
 variable placeholders 14
 vertical bars 13
 WORD 14
 X::X:X 14
 X::X:X/M 14
 XX:XX:XX:XX:XX 14
 configure
 IGMP snooping 63
 configure mode 19
 configuring BSR
 BSR topology 52
 validation commands 53
 configuring RP dynamically 50
 configuring RP statically 47, 96
 curly brackets
 command syntax 13

D

data flow
 PIM-SM 44
 debug igmp 123, 157
 debug ip pim timer joinprune 185, 187
 debug pim packet 179
 debug pim sparse-mode timer register 187
 designated router priority 208
 downstream 44, 59, 67

E

exec command mode 19

G

group-to-RP mappings 52

I

IFNAME 14
 IGMP Commands
 clear ip igmp 122
 debug igmp 123, 157
 ip igmp 125
 ip igmp access-group 126
 ip igmp immediate-leave 127
 ip igmp last-member-query-count 129
 ip igmp last-member-query-interval 130
 ip igmp limit 131
 ip igmp mroute-proxy 132
 ip igmp proxy-service 134
 ip igmp querier-timeout 136
 ip igmp query-interval 137
 ip igmp query-max-response-time 138
 ip igmp robustness-variable 140

- ip igmp snooping 158
 - ip igmp snooping fast-leave 159
 - ip igmp snooping mrouter 160
 - ip igmp snooping querier 161
 - ip igmp snooping report-suppression 162
 - ip igmp ssm-map enable 141
 - ip igmp ssm-map static 142
 - ip igmp static-group 143
 - ip igmp version 146
 - show ip igmp groups 148
 - show ip igmp interface 150
 - show ip igmp snooping mrouter 164
 - show ip igmp snooping statistics 170
 - IGMP snooping
 - configuration 63
 - interface mode 19
 - ip igmp 125
 - ip igmp access-group 126
 - ip igmp immediate-leave 127
 - ip igmp last-member-query-count 129
 - ip igmp last-member-query-interval 130
 - ip igmp limit 131
 - ip igmp mroute-proxy 132
 - ip igmp proxy-service 134
 - ip igmp querier-timeout 136
 - ip igmp query-interval 137
 - ip igmp query-max-response-time 138
 - ip igmp robustness-variable 140
 - ip igmp snooping 158
 - ip igmp snooping fast-leave 159
 - ip igmp snooping mrouter 160
 - ip igmp snooping querier 161
 - ip igmp snooping report-suppression 162
 - ip igmp ssm-map enable 141
 - ip igmp ssm-map static 142
 - ip igmp static-group 143
 - ip igmp version 146
 - ip mroute 108
 - ip msdp default-peer 188
 - ip msdp mesh-group 189
 - ip msdp originator-id 190
 - ip msdp password 191
 - ip msdp peer 192
 - ip multicast route-limit command 109
 - ip multicast ttl-threshold 110
 - ip multicast-routing 111
 - ip pim accept-register list 194
 - ip pim anycast-rp 196
 - ip pim bsr-border 202, 204
 - ip pim bsr-candidate 205
 - ip pim cisco-register-checksum 206
 - ip pim dr-priority 187
 - ip pim exclude-genid 210
 - ip pim hello-holdtime 211
 - ip pim hello-interval 212
 - ip pim ignore-rp-set-priority 213
 - ip pim jp-timer 214
 - ip pim neighbor-filter 215
 - ip pim register-candidate 226
 - ip pim register-rate limit 218
 - ip pim register-rp-reachability 220
 - ip pim register-source 221
 - ip pim rp-address 224
 - ip pim spt-threshold 228
 - ip pim ssm 229
 - ip pim unicast-bsm 231
 - IPv4 address
 - command syntax 14
 - IPv6 address
 - command syntax 14
 - ipv6 mroute 112
- ## L
- LINE 14
- ## M
- MAC address
 - command syntax 14
 - MRIB 43
 - MSDP 75
 - Multicast Commands
 - clear ip mroute 106
 - debug ip mrib
 - debug ip mrib 107
 - ip mroute 108
 - ip multicast route-limit 109
 - ip multicast ttl-threshold 110
 - ip multicast-routing 111
 - show ip mroute 114
 - show ip mvif 117
 - multicast routing 111
 - multicast routing table, displaying 240
- ## N
- nexthop 59
- ## P
- parentheses
 - command syntax 13
 - parentheses
 - command syntax 13
 - period
 - command syntax 14
 - PIM-DM configuration 35, 59
 - downstream 59, 67
 - forwarding multicast packets 59
 - nexthop 59
 - Reverse Path Forwarding 59
 - terminology 67
 - upstream 59, 67
 - PIM-SM commands
 - clear ip mroute 173
 - clear ip msdp sa-cache 176
 - clear ip pim sparse-mode bsr 177

debug ip pim timer joinprune 185, 187
 debug pim packet 179
 debug pim sparse-mode timer register 187
 ip msdp default-peer 188
 ip msdp mesh-group 189
 ip msdp originator-id 190
 ip msdp password 191
 ip msdp peer 192
 ip pim accept-register list 194
 ip pim anycast-rp 196
 ip pim bsr-border 202, 204
 ip pim bsr-candidate 205
 ip pim cisco-register-checksum 206
 ip pim dr-priority 187
 ip pim exclude-genid 210
 ip pim hello-holdtime 211
 ip pim hello-interval 212
 ip pim ignore-rp-set-priority 213
 ip pim jp-timer 214
 ip pim neighbor-filter 215
 ip pim register-rate limit 218
 ip pim register-rp-reachability 220
 ip pim register-source 221
 ip pim rp-address 224
 ip pim rp-candidate 226
 ip pim ssm 229
 ip pim unicast-bsm 231
 show debugging pim 232
 show ip msdp sa-cache 235
 show ip pim bsr-router 237
 show ip pim rp-hash 249
 PIM-SM configuration 43
 bootstrap router 44
 configuring RP dynamically 50
 configuring RP statically 47, 96
 data flow from source to receivers 44
 determining the RP 44
 downstream 44
 electing a designated router 44
 forwarding multicast packets 45
 group-to-RP mappings 52
 joining the shared tree 45
 Multicast Routing Information Base 43
 pruning the interface 45
 references 43
 registering with the RP 45
 rendezvous point 43
 reverse path forwarding 43, 67
 sending out Hello messages 44
 sending Register-Stop messages 45
 shared trees 44
 source-based trees 44
 tree information base 43
 upstream 43
 PIMv4 Commands 171
 privileged exec mode 19

Q

question mark
 command syntax 14

R

references
 PIM-SM 43
 Rendezvous Point 43
 rendezvous point
 mappings 250
 Reverse Path Forwarding 43, 59, 67
 root of the tree 43
 router mode 19
 RP 43
 RPF 43, 59, 67, 75

S

shared trees 44
 show commands 16
 exclude modifier 17
 include modifier 17
 redirect modifier 18
 show debugging pim 232
 show ip igmp groups 148
 show ip igmp interface 150
 show ip igmp snooping mrouter 164
 show ip igmp snooping statistics 170
 show ip mroute 114
 show ip msdp sa-cache 235
 show ip mvif 117
 show ip pim bsr-router 237
 show ip pim rp-hash 249
 show running-config interface igmp 155
 show running-config interface multicast 119
 source-based trees 44
 square brackets
 command syntax 14

T

terminology
 PIM-DM 67
 TIB 43
 time
 command syntax 14
 Tree Information Base 43

V

vertical bars
 command syntax 13

W

WORD 14

