

Multicast Command Reference for Cisco 8000 Series Routers

First Published: 2020-03-15

Last Modified: 2026-09-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface ix

Preface ix

Changes to This Document ix

Communications, Services, and Additional Information ix

CHAPTER 1

IGMP Commands 1

access-group (IGMP) 2

clear igmp counters 3

clear igmp group 5

clear igmp reset 7

explicit-tracking 8

join-group 10

maximum groups 12

maximum groups-per-interface 15

nsf lifetime (IGMP) 19

query-interval 21

query-max-response-time 23

query-timeout 25

robustness-count 27

router 28

router igmp 30

show igmp groups 31

show igmp nsf 33

show igmp nsr 35

show igmp ssm map 37

show igmp summary 38

show igmp traffic 41
show igmp vrf vrf_name groups 44
ssm map 45
static-group 46
version 48
vrf (igmp) 50

CHAPTER 2 Multicast Source Discovery Protocol Commands 51
cache-sa-state 52
cache-sa holdtime 54
clear msdp peer 55
clear msdp sa-cache 56
clear msdp stats 57
connect-source 58
default-peer 60
description (peer) 61
maximum external-sa 62
maximum peer-external-sa 64
mesh-group (peer) 65
global maximum external-sa 66
originator-id 67
password (peer) 68
peer (MSDP) 70
remote-as (multicast) 71
sa-filter 72
show msdp globals 74
show msdp nsr 76
show msdp peer 77
show msdp rpf 79
show msdp sa-cache 81
show msdp statistics peer 85
show msdp summary 87
shutdown (MSDP) 89
show msdp vrf context 90

ttl-threshold (MSDP) 92

CHAPTER 3 **Multicast PIM Commands** 93

accept-register 95

auto-rp candidate-rp 96

bsr candidate-bsr 98

bsr candidate-rp 100

clear pim counters 102

clear pim topology 105

dr-priority 107

global maximum 108

global maximum bsr crp-cache threshold 109

global maximum group-mappings bsr threshold 111

hello-interval (PIM) 113

interface (PIM) 115

join-prune-interval 117

join-prune-mtu 118

maximum register-states 119

maximum route-interfaces 120

maximum routes 121

mofrr 122

neighbor-check-on-recv enable 124

neighbor-check-on-send enable 125

neighbor-filter 126

nsf lifetime (PIM) 127

old-register-checksum 128

router pim 129

rp-address 130

rpf topology route-policy 132

rpf-redirect 133

rpf-redirect bundle 134

rp-static-deny 136

rpf-vector 137

rpf-vector use-standard-encoding 138

show auto-rp candidate-rp 139
show pim global summary 141
show pim nsr 143
show pim rpf-redirect 145
show pim rpf-redirect route 146
show pim segment-database 147
show pim context 149
show pim context table 152
show pim group-map 154
show pim interface 156
show pim join-prune statistic 159
show pim mstatic 161
show pim neighbor 163
show pim nsf 166
show pim range-list 168
show pim rpf 170
show pim rpf hash 172
show pim rpf route-policy statistics 174
show pim rpf route-policy test 176
show pim rpf summary 178
show pim summary 180
show pim topology 182
show pim topology detail 188
show pim topology entry-flag 191
show pim topology interface-flag 193
show pim topology summary 195
show pim traffic 197
show pim tunnel info 199
show pim vrf vrf_name rpf 201
show pim vrf vrf_name topology 202
spt-threshold infinity 203
ssm 204

CHAPTER 4 **Multicast Routing Forwarding Commands** 207

accounting per-prefix 209
address-family (multicast) 211
clear mfib counter 214
clear mfib database 215
clear mfib platform 216
disable (multicast) 218
enable (multicast) 220
forwarding-latency 222
hw-module route-stats 223
hw-module multicast route-scale 225
interface-inheritance disable 226
interface all enable 228
interface (multicast) 230
log-traps 232
maximum disable 233
mdt data ingress replication 234
mdt default ingress replication 235
mdt partitioned ingress replication 236
migration route-policy 237
multicast-routing 238
multipath 239
nsf (multicast) 241
oom-handling 243
rate-per-route 244
route-policy 245
shared-tree-prune delay 246
show mfib connections 247
show mfib counter 249
show mfib encap-info 251
show mfib interface 252
show mfib nsf 254
show mfib platform route 256
show mfib route 260
show mfib table-info 262

show mrib client 264
show mrib mpls forwarding 267
show mrib mpls route 269
show mrib nsf 270
show mrib nsr end 272
show mrib route-collapse 274
show mrib route 276
show mrib route outgoing-interface 279
show mrib table-info 281
show mrib tlc 283
show mrib vrf vrf_name route 284
source-tree-prune-delay 285
static-rpf 286
suppress-pim-data-signaling 288
suppress-shared-tree-join 289
unicast-reachability 290
vrf (multicast) 291

CHAPTER 5 **Hardware Module Commands** 293
Hardware Module Commands 294



Preface

- Preface, on page ix

Preface

The Preface contains these topics:

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

Date	Summary
September 2026	Republished for Release 26.3.1.
June 2026	Republished for Release 26.2.1.
September 2025	Republished for Release 25.3.1.
June 2025	Republished for Release 25.2.1.
March 2025	Republished for Release 25.1.1.
December 2024	Republished for Release 24.4.1.
May 2021	Republished for Release 7.3.15.
March 2020	Initial release of this document for the Release 7.0.12.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



IGMP Commands

- access-group (IGMP), on page 2
- clear igmp counters, on page 3
- clear igmp group, on page 5
- clear igmp reset, on page 7
- explicit-tracking, on page 8
- join-group, on page 10
- maximum groups, on page 12
- maximum groups-per-interface, on page 15
- nsf lifetime (IGMP) , on page 19
- query-interval, on page 21
- query-max-response-time, on page 23
- query-timeout, on page 25
- robustness-count, on page 27
- router, on page 28
- router igmp, on page 30
- show igmp groups, on page 31
- show igmp nsf, on page 33
- show igmp nsr, on page 35
- show igmp ssm map, on page 37
- show igmp summary, on page 38
- show igmp traffic, on page 41
- show igmp vrf vrf_name groups, on page 44
- ssm map, on page 45
- static-group, on page 46
- version, on page 48
- vrf (igmp), on page 50

access-group (IGMP)

To set limits on an interface for multicast-group join requests by hosts, use the **access-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

access-group *access-list*
no access-group *access-list*

Syntax Description

access-list	Number or name of a standard IP access list. Range is 1 to 99.

Command Default

No default behavior or values

Command Modes

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If this command is not specified in router Internet Group Management Protocol (IGMP) configuration mode, the interface accepts all multicast join requests by hosts.

Task ID

Task ID	Operations
multicast	read, write

Examples

In the following example, hosts serviced by HundredGigE 0/0/0/24 can join only group 225.2.2.2:

```
Router# configure
Router(config)# ipv4 access-list mygroup permit 225.2.2.2 0.0.0.0
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE  0/0/0/24
Router(config-igmp-default-if)# access-group mygroup
```

Related Commands

Command	Description
ipv4 access-list	Defines a standard IP access list. For information, see

clear igmp counters

To clear IGMP traffic statistics, use the **clear igmp counters** command in EXEC mode.

clear igmp [**ipv4 vrf** *vrf-name* | **vrf** *vrf-name*] **counters**

Syntax Description

ipv4	(Optional) Specifies IPv4 addressing. IPv4 is the default for Internet Group Management Protocol (IGMP) groups.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

After IGMP statistics are cleared, statistics begin incrementing again.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows sample output before and after clearing IGMP traffic statistics:

```
Router# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:00:19

                                   Received        Sent
Valid IGMP Packets                        0          12
Queries                                   0           3
Reports                                   0           9
Leaves                                    0           0
Mtrace packets                            0           0
DVMRP packets                             0           0
PIM packets                               0           0

Errors:
Malformed Packets                                     0
Bad Checksums                                         0
Socket Errors                                         0
Bad Scope Errors                                      0
Auxiliary Data Len Errors 0
Subnet Errors                                         0
Packets dropped due to invalid socket                 0
Packets which couldn't be accessed                    0
Other packets drops                                   0
```

```
Router# clear igmp counters

Router# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:00:12

                                    Received        Sent
Valid IGMP Packets                         0           1
Queries                                    0           1
Reports                                    0           0
Leaves                                     0           0
Mtrace packets                             0           0
DVMRP packets                              0           0
PIM packets                                0           0

Errors:
Malformed Packets                                      0
Bad Checksums                                          0
Socket Errors                                          0
Bad Scope Errors                                       0
Auxiliary Data Len Errors                              0
Subnet Errors                                          0
Packets dropped due to invalid socket                  0
Packets which couldn't be accessed                     0
Other packets drops                                    0
```

Related Commands

Command	Description
show igmp traffic, on page 41	Displays all the Internet Group Management Protocol (IGMP) traffic-related counters.

clear igmp group

To clear Internet Group Management Protocol (IGMP) groups on one or all interfaces, use the **clear igmp group** command in EXEC mode.

clear igmp [**ipv4 vrf** *vrf-name* | **vrf** *vrf-name*] **group** [*ip-address* | *type interface-path-id*]

Syntax Description

ipv4	(Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ip-address	(Optional) IP hostname or group address.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If no group address is specified, all IGMP groups are cleared.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

To clear all IGMP groups, use the **clear igmp group** command without using an argument. To clear a particular group, use the *ip-address* or *type interface-path-id* arguments.

The following groups cannot be cleared:

- 224.0.0.2
- 224.0.0.13
- 224.0.0.22
- 224.0.0.40

Task ID

Task ID	Operations
multicast	execute

Examples

The following example uses the **show igmp group** command to display the IGMP Connected Group Membership, the **clear igmp group** command to clear address 239.1.1.1, and the **show igmp groups** command again to display the updated list.

```
Router# show igmp groups HundredGigE 0/0/0/24

IGMP Connected Group Membership
Group Address   Interface                      Uptime    Expires   Last Reporter
224.0.0.2       HundredGigE0/0/0/24             3w6d      never     10.114.8.44
224.0.0.5       HundredGigE0/0/0/24             3w6d      never     10.114.8.44
224.0.0.6       HundredGigE0/0/0/24             3w6d      never     10.114.8.44
224.0.0.13      HundredGigE0/0/0/24             3w6d      never     10.114.8.44
224.0.0.22      HundredGigE0/0/0/24             3w6d      never     10.114.8.44

Router# clear igmp groups HundredGigE0/0/0/24

Router# show igmp groups HundredGigE0/0/0/24

IGMP Connected Group Membership
Group Address   Interface                      Uptime    Expires   Last Reporter
224.0.0.2       HundredGigE0/0/0/24                3w6d      never     10.114.8.44
224.0.0.5       HundredGigE0/0/0/24                3w6d      never     10.114.8.44
224.0.0.6       HundredGigE0/0/0/24                3w6d      never     10.114.8.44
224.0.0.13      HundredGigE0/0/0/24                3w6d      never     10.114.8.44
224.0.0.22      HundredGigE0/0/0/24               3w6d      never     10.114.8.44
```

Related Commands

Command	Description
show igmp groups, on page 31	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

clear igmp reset

To clear all Internet Group Management Protocol (IGMP) membership entries and reset connection in the Multicast Routing Information Base (MRIB), use the **clear igmp reset** command in EXEC mode.

clear igmp [**ipv4 vrf** *vrf-name* | **vrf** *vrf-name*] **reset**

Syntax Description

ipv4	(Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Every IGMP group membership that IGMP learns is downloaded to the MRIB database.

The **clear igmp reset** command is used to clear all information from the IGMP topology table and reset the MRIB connection.

Note This command is reserved to force synchronization of IGMP and MRIB entries when communication between the two components is malfunctioning.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows how to clear the group memberships in MRIB:

```
Router# clear igmp reset
```

Related Commands

Command	Description
show igmp groups, on page 31	Displays the multicast groups that are directly connected to the router and that were learned through IGMP
show mrib route	Displays all route entries in the MRIB table.

explicit-tracking

To configure explicit host tracking under Internet Group Management Protocol (IGMP) Version 3, use the **explicit-tracking** command in the appropriate configuration mode. To disable explicit host tracking, use the **no** form of this command.

explicit-tracking [*access-list* | **disable**]
no explicit-tracking

Syntax Description

access-list	(Optional) Access list that specifies the group range for host tracking.
disable	(Optional) Disables explicit host tracking on a specific interface. This option is available only in interface configuration mode.

Command Default

If this command is not specified in IGMP configuration mode, then explicit host tracking is disabled.

Command Modes

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

By default, IGMP supports Version 3, unless a Version 2 or Version 1 IGMP host message is detected in the network. For backward compatibility, IGMP downgrades to run at the IGMP version level that is installed.

This feature allows the router to achieve minimal leave latencies when hosts leave a multicast group or channel. To monitor IGMP membership of hosts, use the **show igmp groups** command in EXEC mode.

In router configuration mode, the **explicit-tracking** command enables explicit host tracking for all interfaces.To disable explicit tracking for all interfaces, use the **no** form of the command from IGMP configuration mode. To disable the feature on specific interfaces, use the **explicit-tracking** command in interface configuration mode with the **disable** keyword, as shown in the following example.

Note If you configure this command in IGMP VRF configuration mode, parameters are inherited by all new and existing interfaces. However, you can override these parameters on individual interfaces from IGMP interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable explicit host tracking for the access list named router1 on all interfaces and how to disable explicit host tracking for a specific GigabitEthernet interface:

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# explicit-tracking router1
Router(config-igmp)# interface hundredGigE 0/0/0/24
Router(config-igmp-default-if)# explicit-tracking disable
```

Related Commands

Command	Description
show igmp groups, on page 31	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

join-group

To have the router join a multicast group, use the **join-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

join-group *group-address* [*source-address*]
no join-group *group-address* [*source-address*]

Syntax Description

group-address	Address of the multicast group. This is a multicast IP address group in IPv4 format • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .
source-address	(Optional) Source address of the multicast group to include in IPv4 prefixing format • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .

Command Default

No multicast group memberships are predefined. If not specified, include is the default.

Command Modes

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **join-group** command permits the IP packets that are addressed to the group address to pass to the IP client process in the Cisco IOS XR software.

If all the multicast-capable routers that you administer are members of a multicast group, pinging that group causes all routers to respond. This command can be a useful administrative and debugging tool.

Another reason to have a router join a multicast group is when other hosts on the network are prevented from correctly answering IGMP queries. When the router joins the multicast group, upstream devices learn multicast routing table information for that group and keep the paths for that group active.



Caution Joining a multicast group can result in a significant performance impact, because all subscribed multicast packets are punted to the route processor.

Task ID

Task ID	Operations
multicast	read, write

Examples

In the following example, the router joins multicast group 225.2.2.2:

```
Router(config)# router igmp
Router(config-igmp)# interface GigabitEthernet 0/1/0/0
Router(config-igmp-default-if)# join-group 225.2.2.2
```

The **join-group** command can have an include/exclude mode for IGMPv3 interfaces as shown in the following example:

```
Router(config)#router igmp
Router(config-igmp)#int gigabitEthernet 0/5/0/1
RP/0/RSP0/CPU0:router(config-igmp-default-if)#join-group ?
A.B.C.D  IP group address
Router(config-igmp-default-if)#join-group 225.0.0.0 ?
A.B.C.D  Source address to include
exclude  Exclude the only following source address include  Include only the following
source address <cr>
Router(config-igmp-default-if)#join-group 225.0.0.0 10.10.10.10 ?
<cr>
Router(config-igmp-default-if)#join-group 225.0.0.0 ?
A.B.C.D  Source address to include
exclude  Exclude the only following source address
include Include only the following source address <cr>
Router(config-igmp-default-if)#join-group 225.0.0.0
```

Related Commands

Command	Description
ping	Checks host reachability and network connectivity on IP networks. For information, see .

maximum groups

To configure the maximum number of groups used by Internet Group Management Protocol (IGMP) and accepted by a router, use the **maximum groups** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

maximum groups *number*
no maximum groups

Syntax Description

number	Maximum number of groups accepted by a router. Range is 1 to 75000.

Command Default

number : 50000

Command Modes

IGMP configuration

IGMP VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When configuring this command within IGMP VRF configuration mode, you may either use the default (unspecified) VRF or a specific VRF by specifying its name.

The maximum combined number of groups on all interfaces can be 75000. After the maximum groups value is met, all additional memberships learned are ignored. The maximum number includes external and local membership.

The following groups obtain local membership on each interface when multicast is enabled and are added into the group totals for each interface: 224.0.0.13 (for PIM), 224.0.0.22 and 224.0.0.2 (for IGMP).

You cannot use the **maximum groups** command to configure the maximum number of groups below the number of existing groups. For instance, if the number of groups is 39, and you set the maximum number of groups to 10, the configuration is rejected.

The router supports a maximum of 16,000 multicast routes per system.

Furthermore, you can use the **maximum groups per-interface** command to configure the maximum number of groups for each interface accepted by a router.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to display the number of groups (39) and the maximum number of groups configured (50000) . Through use of the **maximum groups** command, a configuration is committed to change the maximum number of groups to 40. Before and after configuration, the **show igmp summary** command is used to confirm the configuration change:

```
Router# show igmp summary

IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2

Interface                 Grp No    Max Grp No
MgmtEth0/RSP0/CPU0/0       0         25000
Loopback0                 4         25000
Bundle-Ether24            3         25000
Bundle-Ether28            3         25000
Bundle-Ether28.1          3         25000
Bundle-Ether28.2          3         25000
Bundle-Ether28.3          3         25000
MgmtEth0/RP1/CPU0/0       0         25000
HundredGigE0/0/0/24       3         25000
HundredGigE0/0/0/25       5         25000
HundredGigE0/0/0/26       5         25000

Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups 65
Router(config-igmp)# commit

Router:May 13 12:26:59.108 : config[65704]: %LIBTARCFG-6-COMMIT : Configuration committed
by user 'cisco'.   Use 'show commit changes 1000000025' to view the changes.

Router# show igmp summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2

Interface                 Grp No    Max Grp No
MgmtEth0/RSP0/CPU0/0      0        25000
Loopback0                 4         25000
Bundle-Ether28            3         25000
Bundle-Ether28.1          3         25000
Bundle-Ether28.2          3         25000
Bundle-Ether28.3          3         25000
MgmtEth0/RP1/CPU0/0       0         25000
HundredGigE0/0/0/25       5         25000
HundredGigE0/0/0/26       5         25000
```

Related Commands

Command	Description
maximum groups-per-interface, on page 15	Configures the maximum number of groups for each interface accepted by a router.

Command	Description
show igmp summary, on page 38	Displays group membership information for Internet Group Management Protocol (IGMP).

maximum groups-per-interface

To configure the maximum number of groups for each interface accepted by a router, use the **maximum groups-per-interface** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

maximum groups-per-interface *number*
no maximum groups-per-interface

Syntax Description

number	Maximum number of groups accepted by a router for each interface. Range is 1 to 40000.

Command Default

number : 20000

Command Modes

IGMP configuration

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The following groups obtain local membership on each interface when multicast is enabled and are added into the group totals for each interface: 224.0.0.13 (for Protocol Independent Multicast [PIM]), 224.0.0.22 and 224.0.0.2 (for Internet Group Management Protocol [IGMP]). The number of groups for each interface reflects both external and local group membership.

Note You cannot use the **maximum groups-per-interface** command to configure the maximum number of groups for each interface below the number of existing groups on an interface. For example, if the number of groups is 39, and you set the maximum number of groups to 10, the configuration is rejected.

When you use the **maximum groups-per-interface** command for a specific interface, it overrides the inheritance property of this command specified under IGMP configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to display the maximum number of groups for each interface. A configuration is committed to change the maximum number of groups for each interface to 12. Before and after configuration, use the **show igmp summary** command to confirm the configuration change:

```
Router# show igmp summary

IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2

Interface                Grp No    Max Grp No
MgmtEth0/RSP0/CPU0/0     0         25000
Loopback0                4         25000
Bundle-Ether28           3         25000
Bundle-Ether28.1         3         25000
Bundle-Ether28.2         3         25000
Bundle-Ether28.3         3         25000
MgmtEth0/RP1/CPU0/0      0         25000
HundredGigE 0/0/0/24     3         25000
HundredGigE 0/0/0/25     5         25000
HundredGigE 0/0/0/26     5         25000
HundredGigE 0/0/0/27     3         25000


Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 5
Router(config-igmp)# commit


Router# show igmp summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2

Interface                Grp No    Max Grp No
MgmtEth0/RSP0/CPU0/0      0         5
Loopback0                4         5
Bundle-Ether28           3         5
Bundle-Ether28.1         3         5
Bundle-Ether28.2         3         5
Bundle-Ether28.3         3         5
MgmtEth0/RP1/CPU0/0      0         5
HundredGigE 0/0/0/24     3         5
HundredGigE 0/0/0/25     5         5
HundredGigE 0/0/0/26     5         5
```

The following example shows how to configure all interfaces with 3000 maximum groups per interface except HundredGigE 0/0/0/24, which is set to 4000:

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 3000
```

```
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# maximum groups-per-interface 4000
IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2

Interface                Grp No    Max Grp No
MgmtEth0/RP0/CPU0/0      0         25000
Loopback0                4         25000
Bundle-POS24             3         25000
Bundle-Ether28           3         25000
Bundle-Ether28.1         3         25000
Bundle-Ether28.2         3         25000
Bundle-Ether28.3         3         25000
MgmtEth0/RP1/CPU0/0      0         25000
HundredGigE 0/0/0/25     3         25000
HundredGigE 0/0/0/26     5         25000
HundredGigE 0/0/0/27     5         25000

Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 5
Router(config-igmp)# commit
Router# show igmp summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2

Interface                Grp No    Max Grp No
MgmtEth0/RP0/CPU0/0      0         5
Loopback0                4         5
Bundle-POS24             3         5
Bundle-Ether28           3         5
Bundle-Ether28.1         3         5
Bundle-Ether28.2         3         5
Bundle-Ether28.3         3         5
MgmtEth0/RP1/CPU0/0      0         5
HundredGigE 0/0/0/24     3         5
HundredGigE 0/0/0/25     5         5
HundredGigE 0/0/0/26     5         5
POS0/1/0/1               5         5
POS0/1/4/2               3         5


Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 3000
```

```
Router(config-igmp)# interface POS 0/4/0/0
Router(config-igmp-default-if)# maximum groups-per-interface 4000
```

Related Commands

Command	Description
maximum groups, on page 12	Configures the maximum number of groups used by Internet Group Management Protocol (IGMP).
show igmp summary, on page 38	Displays group membership information for Internet Group Management Protocol (IGMP).

nsf lifetime (IGMP)

To configure the maximum time for the nonstop forwarding (NSF) timeout on the Internet Group Management Protocol (IGMP) process, use the **nsf lifetime** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

nsf lifetime *seconds*
no nsf lifetime

Syntax Description

seconds	Maximum time for NSF mode. Range is 10 to 3600 seconds.

Command Default

seconds : 60

Command Modes

IGMP configuration

IGMP VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The IGMP NSF process is triggered by the restart of the IGMP process. While in IGMP NSF mode, the Multicast Routing Information Base (MRIB) purges the routes installed by the previous IGMP process when the IGMP NSF process times out.

The IGMP NSF lifetime is the period for IGMP to relearn all the host membership of the attached network through membership queries and reports. During this NSF period, PIM continues to maintain forwarding state for the local members while IGMP recovers their membership reports.

Additionally, IGMP recovers the internal receiver state from Local Packet Transport Services (LPTS) for IP group member applications (including the Session Announcement Protocol (SAP) Listener) and updates the MRIB.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the IGMP NSF timeout value to 120 seconds:

```
RP/0/(config)# router igmp
RP/0/(config-igmp)# nsf lifetime 120
```

Related Commands

Command	Description
nsf (multicast)	Enables NSF capability for the multicast routing system.
nsf lifetime (PIM)	Configures the NSF timeout value for the PIM process.

Command	Description
show igmp nsf, on page 33	Displays the state of NSF operation in IGMP.
show mfib nsf	Displays the state of NSF operation for the MFIB line cards.

query-interval

To configure the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages, use the **queryinterval** command in the appropriate configuration mode. To return to the default frequency, use the **no** form of this command.

query-interval *seconds*
no query-interval

Syntax Description

seconds	Frequency used to send IGMP host-query messages. Range is 1 to 3600.

Command Default

If this command is not specified in interface configuration mode, the interface adopts the query interval parameter specified in IGMP configuration mode.

If this command is not specified in IGMP configuration mode, the query interval time is 60 seconds.

Command Modes

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the attached networks of the router. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups (that is, that the host wants to become a member of the group). Host-query messages are addressed to the all-hosts multicast group, which has the address 224.0.0.1, and has an IP time-to-live (TTL) value of 1.

The designated router for a LAN is the only router that sends IGMP host-query messages:

- For IGMP Version 1 (only), the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Versions 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the query-timeout command), it becomes the querier.

Note Changing the value of the *seconds* argument may severely impact network performance. A short query interval may increase the amount of traffic on the attached network, and a long query interval may reduce the querier convergence time.

Note If you configure the **query-interval** command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

This example shows how to change the frequency at which the designated router sends IGMP host-query messages to 2 minutes:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# query-interval 120
```

Related Commands

Command	Description
hello-interval (PIM)	Configures the frequency of PIM hello messages.
query-timeout	Configures the timeout value before the router takes over as the querier for the interface.
show igmp groups, on page 31	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **querymax-response-time** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

query-max-response-time *seconds*
no query-max-response-time

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. Range is 1 to 12.

Command Default

If this command is not specified in interface configuration mode, the interface adopts the maximum response time parameter specified in IGMP configuration mode.

If this command is not specified in IGMP configuration mode, the maximum response time is 10 seconds.

Command Modes

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **query-max-response-time** command is not supported on IGMP Version 1.

This command is used to control the maximum response time for hosts to answer an IGMP query message. Configuring a value less than 10 seconds enables the router to prune groups much faster, but this action results in network burstiness because hosts are restricted to a shorter response time period.

If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces in interface configuration mode.

Note If the hosts do not read the maximum response time in the query message correctly, group membership might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure a maximum response time of 8 seconds:

```
Router(config)# router igmp
```

```
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# query-max-response-time 8
```

Related Commands

Command	Description
hello-interval (PIM)	Configures the frequency of PIM hello messages.
show igmp groups, on page 31	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the **query-timeout** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

query-timeout *seconds*
no query-timeout

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier. Range is 60 to 300.

Command Default

If this command is not specified in interface configuration mode, the interface adopts the timeout value parameter specified in IGMP VRF configuration mode. If this command is not specified in IGMP VRF configuration mode, the maximum response time is equal to twice the query interval set by the **query-interval** command.

Command Modes

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **query timeout** command is not supported on Internet Group Management Protocol (IGMP) Version 1.

By default, the router waits twice the query interval specified by the **query-interval** command, after which, if the router has heard no queries, it becomes the querier. By default, the query interval is 60 seconds, which means that the **query timeout** value defaults to 120 seconds.

If you configure a query timeout value less than twice the query interval, routers in the network may determine a query timeout and take over the querier without good reason.

Note If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces in interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router to wait 30 seconds from the time it received the last query before it takes over as the querier for the interface:

```
Router(config)# router igmp
```

```
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# query-timeout 30
```

Related Commands

Command	Description
query-interval, on page 21	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.

robustness-count

To set the robustness variable to tune for expected packet loss on a network, use the **robustness-count** command in the appropriate configuration mode. To return to the default setting, use the **no** form of this command.

robustness-count *count*
no robustness-count

Syntax Description

count	Value of the robustness count variable. Range is 2 to 10 packets.

Command Default

Default is 2 packets.

Command Modes

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

IGMP is a soft-state protocol. State must be periodically refreshed or it times out. At a **robustness-count** command setting, for example, of 4, a network might lose three IGMP packets related to some specific state yet still maintain the state. If, however, a network lost more than three IGMP packets in the sequence, the state would time out. You might then consider changing the **robustness-count** setting to maintain state.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example illustrates the use of the **robustness-count** command:

```
RP/0/(config)# configure
RP/0/(config)# router igmp
RP/0/(config-igmp)# robustness-count 2
```

router

To disable or enable Internet Group Management Protocol (IGMP) membership tracking, use the **router** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

router {**disable** | **enable**}
no router {**disable** | **enable**}

Syntax Description

disable	Turns off IGMP membership tracking.
enable	Turns on IGMP membership tracking.

Command Default

If this command is not specified in IGMP VRF configuration mode, router functionality is enabled on all interfaces.

Command Modes

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **router** command is used to enable and disable the IGMP router functionality on a specific interface. For instance, IGMP stops queries from an interface when the router functionality is disabled on that interface. Disabling IGMP router functionality does not prevent local group membership from being announced through the group membership report.

Note This command is useful if you want to disable or enable IGMP interfaces that have been previously enabled through the **multicast-routing** command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable IGMP membership tracking functionality on all multicast enabled interfaces, except Packet-over-SONET/SDH (POS) interface HundredGigE 0/0/0/24:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# router enable
```

Related Commands

Command	Description
multicast routing	Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.

router igmp

To enter Internet Group Management Protocol (IGMP) configuration mode, use the **router igmp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

router igmp
no router igmp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Default

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

From IGMP VRF configuration mode, you can configure the maximum response time advertised in IGMP queries and modify the host query interval.

Note The IGMP process is turned on when the **router igmp** command or the **multicast-routing** command is initiated.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enter IGMP configuration mode:

```
Router(config)# router igmp
Router(config-igmp)#
```

Related Commands

Command	Description
interface all disable	Disables IGMP membership tracking on all interfaces.
multicast routing	Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.

show igmp groups

To display the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show igmp groups** command in EXEC mode.

show igmp [**vrf** *vrf-name*] **groups** [*group-address* | *type interface-path-id* | **not-active** | **summary**] [**detail**] [**explicit**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
group-address	(Optional) Address or name of the multicast group. An address is a multicast IP address in four-part dotted-decimal notation. A name is as defined in the Domain Name System (DNS) hosts table.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Either a physical interface or a virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
not-active	(Optional) Displays group joins that are not processed.
summary	(Optional) Displays the total number of (* , G) and (S, G) states in IGMP.
detail	(Optional) Displays detail information such as IGMP Version 3 source list, host, and router mode.
explicit	(Optional) Displays explicit tracking information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you omit all optional arguments, the **show igmp groups** command displays (by group address and interface name) all the multicast memberships that the directly connected networks have subscribed.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show igmp groups** command on a specific (HundredGigE) interface:

```
Router# show igmp groups HundredGigE 0/0/0/24

IGMP Connected Group Membership
Group Address   Interface                      Uptime    Expires   Last Reporter
224.0.0.2       HundredGigE 0/0/0/24            3w6d      never     10.114.8.44
224.0.0.5       HundredGigE 0/0/0/24            3w6d      never     10.114.8.44
224.0.0.6       HundredGigE 0/0/0/24            3w6d      never     10.114.8.44
224.0.0.13      HundredGigE 0/0/0/24            3w6d      never     10.114.8.44
224.0.0.22      HundredGigE 0/0/0/24            3w6d      never     10.114.8.44
```

This table describes the significant fields shown in the display.

Table 2: show igmp groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry is removed from the IGMP groups table.
Last Reporter	Last host to report being a member of the multicast group.

show igmp nsf

To display the state of the nonstop forwarding (NSF) operation in Internet Group Management Protocol (IGMP), use the **show igmp nsf** command in EXEC mode

.

show igmp [**vrf** *vrf-name*] **nsf**

Syntax Description

old-output	(Optional) Displays the old show output—available for backward compatibility.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show igmp nsf** command displays the current multicast NSF state for IGMP. The NSF state that is displayed may be either normal or activated for NSF. The activated state indicates that recovery is in progress due to an IGMP failure. The total NSF timeout and time remaining are displayed until NSF expiration.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show igmp nsf** command:

```
RP/0/# show igmp nsf

IGMP_AFD
Non-Stop Forwarding Status: Multicast routing state: Normal


NSF Lifetime
:       00:01
:00
```

This table describes the significant fields shown in the display.

Table 3: show igmp nsf Field Descriptions

Field	Description
Multicast routing state	Multicast NSF status of IGMP (Normal or Non-Stop Forwarding Activated).

Field	Description
NSF Lifetime	Timeout for IGMP NSF. IGMP remains in the NSF state, recovering the IGMP route state through IGMP reports for this period of time, before making the transition back to the normal state and signaling the Multicast Routing Information Base (MRIB).
NSF Time Remaining	If IGMP NSF state is activated, the time remaining until IGMP reverts to Normal mode displays.

Related Commands

Command	Description
nsf (multicast)	Enables NSF capability for the multicast routing system.
nsf lifetime (IGMP)	Configures the NSF timeout value for the IGMP or MLD process. Configures the NSF timeout value for the IGMP process.
nsf lifetime (PIM)	Configures the NSF timeout value for the PIM process.
show mfib nsf	Displays the state of NSF operation for the MFIB line cards.
show mrib nsf	Displays the state of NSF operation in the MRIB.
show pim nsf	Displays the state of NSF operation for PIM.

show igmp nsr

To display the nonstop routing (NSR) information in Internet Group Management Protocol (IGMP), use the **show igmp nsr** command in EXEC mode.

show igmp ipv4| ipv6 nsr

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show igmp nsr** command displays the current multicast NSR information for IGMP. The NSR state that is displayed may be either normal or activated for NSR. The activated state indicates that recovery is in progress due to an IGMP failure. The total NSR timeout and time remaining are displayed until NSR expiration.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show igmp nsr** command:

```
Router# show igmp nsr

IGMP NSR Data :-
NSR State                      : Not Ready (uptime 4w0d)
Converged with collaborators   : Y
Partner connection state       : Not-coverged/Down
RMF Notif done                 : Y
Last RMF ready notified        : Never [0]
Last RMF not ready notifed     : 4w0d [1]
Last partner process conn up   : Never [0]
Last partner process conn down : Never [0]
```

This table describes the significant fields shown in the display.

Table 4: show igmp nsr Field Descriptions

Field	Description
NSR State	Multicast Non-Stop Routing State: Ready or Not Ready

Field	Description
Converged with collaborators	Yes or No
Partner connection state	Converged/Yes or Non-converged/No
RMF Notif done	RMF notification whether activated: Yes or No
Last RMF ready notified	The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF ready notification was received.
Last RMF not ready notified	The Time when the last RMF not ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF ready notification was received.

Related Commands

Command	Description
show msdp nsr	Displays the state of NSR operation for MSDP.
show mrib nsr	Displays the state of NSR operation in MRIB.
show pim nsr	Displays the state of NSR operation for PIM.

show igmp ssm map

To query the source-specific mapping (SSM) state, use the **show igmp ssm map** command in EXEC mode.

show igmp [**vrf** *vrf-name*] **ssm map** [*group-address*] [**detail**]

Syntax Description

vrf	(Optional) Specifies a VPN routing and forwarding (VRF) instance to be queried.
vrf-name	(Optional) Specifies the name of the specific VRF instance.
group-address	(Optional) Specifies the address of the SSM group for which to obtain the mapping state.
detail	(Optional) Displays detailed source information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following example illustrates the use of the **show igmp ssm map** command:

```
Router# show igmp ssm map 232.1.1.1

232.1.1.1 is static with 1 source
```

show igmp summary

To display group membership information for Internet Group Management Protocol (IGMP), use the **show igmp summary** command in EXEC mode.

show igmp [**vrf vrf-name**] **summary**

Syntax Description

old-output	(Optional) Displays the old show output—available for backward compatibility.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show igmp summary** command is used to display the total group membership. The value for number of groups is the total number of group members on all interfaces. The value for maximum number of groups is the total number of external and local members possible for all interfaces. The maximum number of groups and the default value for the maximum number of groups is 50000 members. The maximum number of groups for each interface, and the default value for the maximum number of groups for each interface, is 25000 members.

Task ID

Task ID	Operations
multicast	read

Examples

The following example shows the number of groups for each interface that are IGMP members and the maximum number of groups that can become members on each interface:

```
Router# show igmp summary

IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces     : 18
Disabled Interfaces    : 2


Interface

Grp No
```

```
 Max Grp No
Bundle-Ether28.1          3          5
MgmtEth0/RSP0/CPU0/0

0
        5
Loopback0

        4
        5
MgmtEth0/RP1/CPU0/0       0          5
Bundle-Ether28
   3         5
Bundle-Ether28

3
        5
Bundle-Ether28.1

3
        5
Bundle-Ether28.2

3
        5
Bundle-Ether28.3
         3         5
MgmtEth0
/RP1
/CPU0
/0

    0
        5
GigabitEthernet0/1
/5/0
   3         5
GigabitEthernet0/1
/5/1

5
        5
```

This table describes the significant fields shown in the display.

Table 5: show igmp summary Field Descriptions

Field	Description
No. of Group x Interfaces	Number of multicast groups that are joined through the interface.
Maximum number of Group x Interfaces	Maximum number of multicast groups that can be joined through the interface.
Supported Interfaces	Interfaces through which the multicast groups are reachable.
Unsupported Interfaces	Number of unsupported interfaces.
Enabled Interfaces	Number of enabled interfaces.

Field	Description
Disabled Interfaces	Number of disabled interfaces.

Related Commands

Command	Description
show igmp groups, on page 31	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

show igmp traffic

To display all the Internet Group Management Protocol (IGMP) traffic-related counters, use the **show igmp traffic** command in EXEC mode.

show igmp [**vrf vrf-name**] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show igmp traffic** command is used to display the state of all counters for IGMP traffic. It gives information about the length of time the counters have been active and the count of different types of IGMP packets received, such as queries, leaves, and reports. Also, this command keeps a count of all the erroneous IGMP packets received.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show igmp traffic** command:

```
RP/0/# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 15:27:38

                                    Received        Sent
Valid IGMP Packet                       2784        5576
Queries                                    0        2784
Reports                                 2784        2792
Leaves                                     0           0
Mtrace packets                             0           0
DVMRP packets                              0           0
PIM packets                                0           0

Errors:
Malformed Packets                                      0
Bad Checksums                                          0
Socket Errors                                          0
Bad Scope Errors                                       0
Auxiliary Data Len Error                               0
Subnet Errors                                          0
```

```
Packets dropped due to invalid socket             0
Packets which couldn't be accessed                0
```

This table describes the significant fields shown in the display for the **show igmp traffic** command.

Table 6: show igmp traffic Field Descriptions

Field	Description
Valid IGMP Packet	Total number of valid protocol packets sent and received. Valid packet types include: • Queries • Membership reports • Leaves
Queries	Total number of query packets sent and received. IP Multicast routers send queries to determine the multicast reception state of neighboring interfaces.
Reports	Total number of membership report packets received. Membership reports indicate either the current multicast reception state of a neighboring interface or a change to that state.
Leaves	Total number of leaves received. A leave group packet indicates a neighboring interface no longer has multicast reception state for a particular group.
Mtrace packets	Total number of Mtrace packets sent and received. Mtrace traces the route from a receiver to a source using a particular multicast address.
DVMRP packets	Total number of Distance Vector Multicast Routing Protocol (DVMRP) packets sent and received. DVMRP is an Internet routing protocol that provides a mechanism for connectionless datagram delivery to a group of hosts across an internetwork. This protocol dynamically generates IP multicast delivery trees using Reverse Path Multicasting. Packet type 0x13 indicates a DVMRP packet.
PIM packets	Total number of sent and received Protocol Independent Multicast (PIM) packets.
Malformed Packets	Total number of malformed packets received. A malformed packet is a packet smaller than the smallest valid protocol packet.
Bad Checksums	Total number of packets received with a bad protocol header checksum.
Socket Errors	Total number of read and write failures on the protocol socket.
Bad Scope Errors	Total number of packets received with an invalid multicast scope. **Note** IGMP has no invalid scopes; this counter, therefore, never increments in IGMP.
Auxiliary Data Len Errors	Total number of packets received with a non-zero auxilary data length.

Field	Description
Subnet Errors	Total number of packets received that were not sourced on the same subnet as the router. DVMRP and MTRACE packets received are not checked for this error as they may be validly sourced from a different subnet.
Packets dropped due to invalid socket	Total number of packets dropped due to an invalid socket.
Packets which couldn't be accessed	Total number of packets that could not be sent or received. This might occur if: • Packet buffer does not form a valid protocol packet. • IP header is not written to the packet. • Outgoing packet interface handle was not set. • Errors occurred calculating the protocol checksum.
Other Packet Drops	Packets dropped for any other reason.

Related Commands

Command	Description
show pim traffic	Displays PIM traffic counter information.

show igmp vrf vrf_name groups

To display the IGMP group membership information, use the **show igmp vrf** *vrf_name* **groups** command in the EXEC mode.

show igmp vrf *vrf_name* **groups** *ip_address*

Syntax Description

ip_address	Specifies the IP address or group address.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read

```
Router# show igmp vrf vrf1 groups 232.1.1.1
IGMP Connected Group Membership
Group Address   Interface                      Uptime    Expires   Last Reporter
232.1.1.1       tunnel-mte1                    12:39:31  never     110.110.110.110
```

ssm map

To map group memberships from legacy hosts in Source-Specific Multicast (SSM) groups accepted by an access control list (ACL) to a Protocol Independent Multicast (PIM)-SSM source or to configure DNS mapping for PIM-SSM sources to a set of SSM groups, use the **ssm map** command in the appropriate configuration mode. To revert to default behavior, use the **no** form of this command.

ssm map { **static** *source-address access-list* }
no ssm map { **static** *source-address access-list* }

Syntax Description

source-address	PIM-SSM source address to be used to create a static mapping.
access-list	ACL specifying the groups to be used to create a static mapping.

Command Default

Legacy host membership reports in the SSM group range are discarded.

Command Modes

IGMP VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

PIM-SSM requires the use of IGMPv3 (IPv4) to determine local memberships. Under normal operating conditions, IGMP discards older version group membership reports for groups in the SSM group range. This means that a host with a legacy group membership protocol is unable to receive data from a PIM-SSM source.

The **ssm map static** command maps an older group membership report to a set of PIM-SSM sources. If the ACL associated with a configured source accepts the SSM group, then that source is included in its set of sources for the SSM group.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows PIM-SSM mapping in IGMP routing configuration mode:

```
Router(config)# configuration
Router(config)# router igmp
Router(config-igmp)# ssm map static 10.0.0.1 mc2
Router(config-igmp)#
```

static-group

To configure the router to be a statically configured member of the specified group on the interface, or to statically forward for a multicast group onto the interface, use the **static-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

static-group *group-address* [**inc-mask** *mask* **count** *cnt*] [*source-address* [**inc-mask** *mask* **count** *cnt*]]
no static-group *group-address* [**inc-mask** *mask* **count** *cnt*] [*source-address* [**inc-mask** *mask* **count** *cnt*]]

Syntax Description

group-address	IP address of the multicast group in IPv4 prefixing format: • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .
inc-mask *mask*	(Optional) Specifies a mask for the increment range. This is an IP address expressed range in IPv4 format. This mask is used with the group address to generate subsequent group addresses: • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* **Note** This mask is used with the group address to generate subsequent group addresses.
count *cnt*	(Optional) Specifies a number of group addresses to generate using the increment mask. Range is 1 to 512.
source address	(Optional) Source address of the multicast group to include in IPv4 prefixing format: • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .

Command Default

A router is not a statically connected member of an IP multicast group.

Command Modes

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When you configure the **static-group** command, packets to the group are switched out the interface, provided that packets were received on the correct Reverse Path Forwarding (RPF) interface.

The **static-group** command differs from the **join-group** command. The **join-group** command allows the router to join the multicast group and draw traffic to an IP client process (that is, the route processor). If you configure both the **join-group** and **static-group** command for the same group address, the **join-group** command takes precedence and the group behaves like a locally joined group.

Note The **static-group** command has no impact on system performance. Configuring a static-group on a loopback interface has no effect on the router.

Task ID

Task ID	Operations
multicast	read, write

Examples

In the following example, the router statically joins two multicast groups 225.2.2.2 and 225.2.2.4 for the specific source 1.1.1.1:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE  0/0/0/24
Router(config-igmp-default-if)# static-group 225.2.2.2 inc-mask 0.0.0.2 count 2 1.1.1.1
```

version

To configure an Internet Group Management Protocol (IGMP) version for the router, use the **version** command in the appropriate configuration mode. To restore the default value, use the **no** form of this command.

version {**1** | **2** | **3**}
no version

Syntax Description

1	Specifies IGMP Version 1.
2	Specifies IGMP Version 2.
3	Specifies IGMP Version 3.

Command Default

If this command is not specified in interface configuration mode, the interface adopts the IGMP version parameter specified in IGMP VRF configuration mode.

If this command is not specified in IGMP configuration mode, IGMP uses Version 3.

Command Modes

IGMP configuration

IGMP VRF configuration

IGMP interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

All routers on the subnet must be configured with the same version of IGMP. For example, a router running Cisco IOS XR software does not automatically detect Version 1 systems and switch to Version 1. Hosts can have any IGMP version and the router will correctly detect their presence and query them appropriately.

The **query-max-response-time** and **query-timeout** commands require IGMP Version 2 or 3.



Note If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router to use IGMP Version 3:

```
Router(config)# router igmp
Router(config-igmp)# version 3
```

Related Commands

Command	Description
query-max-response-time, on page 23	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.
query-timeout, on page 25	Configures the timeout value before the router takes over as the querier for the interface.

vrf (igmp)

To configure a virtual private network (VRF) instance, use the **vrf** command in IGMP routing configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF instance.

Command Default

No default behavior or values.

Command Modes

IGMP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When you use the **vrf** command from the IGMP routing configuration mode to configure a VRF instance, you enter the IGMP VRF configuration submode.

A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure a VRF instance in IGMP configuration submode and to enter VRF configuration submode:

```
Router(config)# router igmp
Router(config-igmp)# vrf  vrf_1
Router(config-igmp-vrf_1)#
```



Multicast Source Discovery Protocol Commands

- cache-sa-state, on page 52
- cache-sa holdtime, on page 54
- clear msdp peer, on page 55
- clear msdp sa-cache, on page 56
- clear msdp stats, on page 57
- connect-source, on page 58
- default-peer , on page 60
- description (peer), on page 61
- maximum external-sa, on page 62
- maximum peer-external-sa, on page 64
- mesh-group (peer), on page 65
- global maximum external-sa, on page 66
- originator-id, on page 67
- password (peer), on page 68
- peer (MSDP), on page 70
- remote-as (multicast), on page 71
- sa-filter, on page 72
- show msdp globals, on page 74
- show msdp nsr, on page 76
- show msdp peer, on page 77
- show msdp rpf , on page 79
- show msdp sa-cache, on page 81
- show msdp statistics peer, on page 85
- show msdp summary, on page 87
- shutdown (MSDP), on page 89
- show msdp vrf context, on page 90
- ttl-threshold (MSDP), on page 92

cache-sa-state

To control cache source-active (SA) state on a router, use the **cache-sa-state** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

cache-sa-state {**list** *access-list-number* | **rp-list** *access-list-name*}
no cache-sa-state {**list** *access-list-number* | **rp-list** *access-list-name*}

Syntax Description

list *access-list-number*	Specifies an IP access list that defines which (S, G) pairs to cache.
rp-list *access-list-name*	Specifies an access list name for the originating rendezvous point (RP).

Command Default

The router creates SA state.

Command Modes

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When a new member joins a group immediately after an SA message arrives, latency may occur and an SA message may be missed. To overcome this problem, you can configure this command and the router will supply SA information (from cache memory) to the new member instead of requiring that the member wait until the next SA message is received.

The **cache-sa-state** command is required in every Multicast Source Discovery Protocol (MSDP) speaker, to cache SA messages received from peers.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the cache state for all sources in 10.0.0.0/16 sending to groups 224.2.0.0/16:

```
RP/0/# configure
RP/0/(config)# MSDP
RP/0/(config-msdp)# cache-sa-state list 100
RP/0/(config-msdp)# exit
RP/0/(config)# ipv4
access-list 100 permit 10.0.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

Note The source and destination fields in the access list matches on the (S,G) fields in the SA messages. We recommend that the first address and mask field in the access list is used for the source and the second field in the access list is used for the group or destination.

Related Commands

Command	Description
show msdp sa-cache, on page 81	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

cache-sa holdtime

To configure the cache source-active (SA) state hold-time period on a router, use the **cache-sa-holdtime** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

cache-sa-holdtime *holdtime-number*
no cache-sa-holdtime *holdtime-number*

Syntax Description

holdtime-number	Hold-time period (in seconds). Range is 150 to 3600.

Command Default

holdtime-number : 150 seconds

Command Modes

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **cache-sa-holdtime** command is used to increase the cache SA state hold time. Any cache entry that is created usually expires after 150 seconds. For troubleshooting purposes, you may need Multicast Source Discovery Protocol (MSDP) to keep SA cache entries for a longer period.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the cache SA state hold-time period to 200 seconds:

```
RP/0/# configure
RP/0/(config)# router
msdp
RP/0/(config-msdp)# cache-sa-holdtime
200
```

Related Commands

Command	Description
cache-sa-state, on page 52	Controls cache source-active (SA) state on a router.

clear msdp peer

To clear the TCP connection of the specified Multicast Source Discovery Protocol (MSDP) peer, use the **clear msdp peer** command in EXEC mode.

clear msdp [**ipv4**] **peer** *peer-address*

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
peer-address	IPv4 address or hostname of the MSDP peer to which the TCP connection is cleared.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **clear msdp peer** command closes the TCP connection to the MSDP peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows how to clear the TCP connection of the MSDP peer at address 224.15.9.8:

```
RP/0/# clear msdp peer 224.15.9.8
```

Related Commands

Command	Description
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.

clear msdp sa-cache

To clear external Multicast Source Discovery Protocol (MSDP) source-active (SA) cache entries, use the **clear msdp sa-cache** command in EXEC mode.

clear msdp [**ipv4**] **sa-cache** [*group-address*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
group-address	(Optional) Multicast group address or name for which external SA entries are cleared from the SA cache.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Note SA caching is enabled by default on Cisco IOS XR software.

If you do not specify a multicast group by group address or group name with the *group-address* argument, the **clear msdp sa-cache** command clears all external SA cache entries.

Note Local SA cache entries can be cleared using the **clear pim topology** command.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows how to clear the external SA entries for the multicast group at address 224.5.6.7 from the cache:

```
RP/0/# clear msdp sa-cache 224.5.6.7
```

Related Commands

Command	Description
show msdp sa-cache, on page 81	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

clear msdp stats

To reset Multicast Source Discovery Protocol (MSDP) peer statistic counters, use the **clear msdp stats** command in EXEC mode.

clear msdp [**ipv4**] **stats** [**peer** *peer-address*] [**allvalues**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
peer *peer-address*	(Optional) Clears MSDP peer statistic counters for the specified IPv6 MSDP peer address or peer name.
allvalues	(Optional) Clears all statistic counters for all MSDP peers.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **clear msdp stats** command resets MSDP peer statistic counters such as the number of keepalives sent and received and the number of Source Active (SA) entries sent and received.

If you do not specify an MSDP peer with the **peer** keyword and *peer-address* argument, this command clears statistic counters for all MSDP peers.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows how to clear all statistics for all peers:

```
RP/0/# clear msdp stats peer 224.0.1.1
```

Related Commands

Command	Description
show msdp statistics peer, on page 85	Displays Multicast Source Discovery Protocol (MSDP) peer statistic counters.

connect-source

To configure a source address used for a Multicast Source Discovery Protocol (MSDP) connection, use the **connect-source** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

connect-source *type* [*interface-path-id*]
no connect-source *type* [*interface-path-id*]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If a source address is not configured for the MSDP connection, the IP address of the interface toward the peer is used as a source address.

Command Modes

MSDP configuration

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **connect-source** command:

- Specifies the interface type and path ID whose primary address becomes the source IP address for the TCP connection.
- Is recommended for MSDP peers that peer with a router inside the remote domain.
- Can be configured globally for MSDP (and is inheritable by MSDP peers). This global configuration can be overridden if the command is issued again in peer configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure a loopback interface source address for an MSDP connection:

```
RP/0/(config)# interface loopback 0
```

```
RP/0/(config-if)# ipv4 address 10.1.1.1/24
RP/0/(config-if)# exit
RP/0/(config)# router msdp
RP/0/(config-msdp)# connect-source loopback 0
```

default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) source-active (SA) messages, use the **default-peer** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

default-peer *ip-address*
no default-peer

Syntax Description

ip-address	IP address or Domain Name System (DNS) name of the MSDP default peer.

Command Default

No default MSDP peer exists.

Command Modes

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A default peer configuration accepts all MSDP Source-Active (SA) messages, as a last Reverse Path Forwarding (RPF) rule, when all other MSDP RPF rules fail.

Use the **default-peer** command if you do not want to configure your MSDP peer to be a BGP peer also.

When the **prefix-list** *list* keyword and argument are not specified, all SA messages received from the configured default peer are accepted.

Remember to configure a BGP prefix list to configure the **prefix-list** *list* keyword and argument with the **default-peer** command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router 172.16.12.0 as the default peer to the local router:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# default-peer 172.16.12.0
```

Related Commands

Command	Description
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.

description (peer)

To add descriptive text to the configuration for a Multicast Source Discovery Protocol (MSDP) peer, use the **description** command in peer configuration mode. To return to the default behavior, use the **no** form of this command.

description *peer-address text*
no description *peer-address text*

Syntax Description

peer-address	IP address or hostname for the peer to which this description applies.
text	Description of the MSDP peer. Use up to 80 characters to describe this peer.

Command Default

No description is associated with an MSDP peer.

Command Modes

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Configure a description to make the MSDP peer easier to identify. This description is visible in the **show msdp peer** command output.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router at the IP address 10.0.5.4 with a description indicating that it is a router at customer site A:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 10.0.5.4
RP/0/(config-msdp-peer)# description 10.0.5.4 router_at_customer_site_A
```

Related Commands

Command	Description
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.
show msdp peer, on page 77	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.

maximum external-sa

To configure the maximum number of external Multicast Source Discovery Protocol (MSDP) source-active (SA) entries that can be learned by the router or by a specific MSDP peer, use the **maximum external-sa** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

maximum external-sa *entries*
no maximum external-sa

Syntax Description

entries	Maximum number of SA entries that can be learned by the router or a specific MSDP peer. Range is 1 to 75000.

Command Default

entries : 20000

Command Modes

MSDP peer configuration

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When issued from MSDP configuration mode, the **maximum external-sa** command configures the total number of external SA entries (that is, the total cumulative SA state for all peers) that can be learned by the router. This command is used to control router resource utilization under heavy traffic conditions.

Note The configuration fails if you configure the maximum number of external SA entries to be lower than the current accumulated SA state.

When issued from MSDP peer configuration mode, the **maximum external-sa** command configures the total number of external SA entries that can be learned by a specific MSDP peer. From MSDP configuration mode, this command can also be used to configure a specific MSPD peer to override the maximum external SA entry value configured with the **maximum peer-external-sa** command.

Note The configuration fails if you configure the maximum number of external SA entries for a specific MSDP peer to be higher than the maximum number of external SA entries that can be learned by the router.

Task ID

Task ID	Operations
multicast	read, write

Examples

This example shows how to configure the maximum number of external SA entries that can be learned by the router to 30000 SA entries:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# maximum external-sa 30000
```

This example shows how to configure the maximum number of external SA entries that can be learned by the MSDP peer at address 10.1.5.3 to 25000 SA entries:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 10.1.5.3
RP/0/(config-msdp-peer)# maximum external-sa 25000
```

Related Commands

Command	Description
maximum peer-external-sa, on page 64	Configures the maximum number of external Multicast Source Discovery Protocol (MSDP) Source-Active (SA) entries that can be learned from MSDP peers.
show msdp summary, on page 87	Displays Multicast Source Discovery Protocol (MSDP) peer status.

maximum peer-external-sa

To configure the maximum number of external Multicast Source Discovery Protocol (MSDP) Source-Active (SA) entries that can be learned from MSDP peers, use the **maximum peer-external-sa** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

maximum peer-external-sa *entries*
no maximum peer-external-sa

Syntax Description

entries	Maximum number of SA entries to be learned by MSDP peers. Range is 1 to 75000.

Command Default

entries : 20000

Command Modes

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **maximum peer-external-sa** command configures the maximum number of external SA entries that can be learned for each configured MSDP peer, whereas the **maximum external-sa** command (in MSDP configuration mode) configures the maximum number of SA entries accepted by the router as a cumulative total.

Note The configuration fails if you attempt to configure the maximum number of external SA entries for MSDP peers to be higher than the maximum number of external SA entries that can be learned by the router.

Task ID

Task ID	Operations
multicast	read, write

Examples

This example shows how to configure the maximum number of external SA entries that each MSDP peer can learn to 27000 SA entries:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# maximum peer-external-sa 27000
```

Related Commands

Command	Description
maximum external-sa, on page 62	Configures the maximum number of external Multicast Source Discovery Protocol (MSDP) source-active (SA) entries that can be learned by the router or by a specific MSDP peer.
show msdp summary, on page 87	Displays Multicast Source Discovery Protocol (MSDP) peer status.

mesh-group (peer)

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **mesh-group** command in peer configuration mode. To return to the default behavior, use the **no** form of this command.

mesh-group *name*
no mesh-group *name*

Syntax Description

name	Name of the mesh group.

Command Default

MSDP peers do not belong to a mesh group.

Command Modes

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A *mesh group* is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. Any Source-Active (SA) messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group.

Mesh groups can be used to:

- Reduce SA message flooding
- Simplify peer Reverse Path Forwarding (RPF) flooding (no need to run Border Gateway Protocol [BGP] among MSDP peers)

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the MSDP peer at address 10.0.5.4 to be a member of the mesh group named internal:

```
RP/0/# configure
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 10.0.5.4
RP/0/(config-msdp-peer)# mesh-group internal
```

global maximum external-sa

To limit the total number of source active (SA) messages across all VRFs, use the **global maximum external-sa** command in the MSDP configuration mode. To remove the set SA messages limit use the **no** form of the command.

global maximum external-sa *value*
no global maximum external-sa

Syntax Description

value	Specifies the maximum-limit for the source active messages. Range is 1 to 75000.

Command Default

None

Command Modes

MSDP configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The value configured using the **global maximum external-sa** command must be greater than the maximum value of any VRF, which, in turn, must be greater than the maximum value of any peer in that VRF. When the set limit is reached, a syslog message is issued.

Task ID

Task ID	Operation
multicast	read, write

This example shows the maximum-limit value for the source active messages, set to 100:

```
RP/0/ (config-msdp) # global maximum external-sa 100
```

originator-id

To identify an interface type and instance to be used as the rendezvous point (RP) address in a Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message, use the **originator-id** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

originator-id *type interface-path-id*
no originator-id *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

The RP address is used as the originator ID.

Command Modes

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **originator-id** command allows an MSDP speaker that originates an SA message to use the IP address of the interface as the RP address in the SA message.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure Gigabit Ethernet interface 0/1/1/0 to be used as the RP address in SA messages:

```
Route(config)# router msdp
Router(config-msdp)# originator-id HundredGigE0/0/0/24
```

password (peer)

To enable Message Digest 5 (MD5) authentication on a TCP connection between two Multicast Source Discovery Protocol (MSDP) peers, use the **password** command in MSDP peer configuration mode. To return to the default behavior, use the **no** form of this command.

password {**clear** | **encrypted**} *password*
no password {**clear** | **encrypted**} *password*

Syntax Description

clear	Specifies that an unencrypted password follows. The password must be a case-sensitive, clear-text unencrypted password.
encrypted	Specifies that an encrypted password follows. The password must be a case-sensitive, encrypted password.
password	Password of up to 80 characters. The password can contain any alphanumeric characters. However, if the first character is a number or the password contains a space, the password must be enclosed in double quotation marks; for example, "2 password."

Command Default

No password is configured.

Command Modes

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **password** command supports MD5 signature protection on a TCP connection between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them is not made. Configuring MD5 authentication causes the Cisco IOS XR software to generate and verify the MD5 digest of every segment sent on the TCP connection.

Use the **show msdp peer** command to check if a password has been configured on a peer.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the MSDP password on a peer:

```
RP/0/# configure
RP/0/(config)# router msdp
```

```
RP/0/(config-msdp)# peer 10.0.5.4
RP/0/(config-msdp-peer)# password encrypted a34bi5m
```

Related Commands

Command	Description
show msdp peer, on page 77	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.

peer (MSDP)

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the **peer** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

peer *peer-address*
no peer *peer-address*

Syntax Description

peer-address	IP address or Domain Name System (DNS) name of the router that is to be the MSDP peer.

Command Default

No MSDP peer is configured.

Command Modes

MSDP configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Configure the specified router as a Border Gateway Protocol (BGP) neighbor.

If you are also BGP peering with this MSDP peer, use the same IP address for MSDP as you do for BGP. However, you are not required to run BGP with the MSDP peer, as long as there is a BGP path between the MSDP peers. If there is no path, you must configure the **default-peer** command from MSDP configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router at the IP address 172.16.1.2 as an MSDP peer to the local router and enter MSDP peer configuration mode:

```
RP/0/# configure
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 172.16.1.2
RP/0/(config-msdp-peer)#
```

Related Commands

Command	Description
default-peer , on page 60	Defines a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) source-active (SA) messages.

remote-as (multicast)

To configure the remote autonomous system number of this peer, use the **remote-as** command in peer configuration mode. To return to the default behavior, use the **no** form of this command.

remote-as *as-number*
no remote-as *as-number*

Syntax Description

as-number	Autonomous system number of this peer. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.

Command Default

If this command is not issued during peer configuration, the remote autonomous system value is derived from BGP (if also configured) or initialized to zero, when only Interior Gateway Protocol (IGP) is present.

Command Modes

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **remote-as** command to configure remote autonomous system if deriving the autonomous system value from the configured Border Gateway Protocol (BGP) is not required.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the autonomous system number for the specified peer to 250:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 172.16.5.4
RP/0/(config-msdp-peer)# remote-as 250
```

sa-filter

To configure an incoming or outgoing filter list for Source-Active (SA) messages received from the specified Multicast Source Discovery Protocol (MSDP) peer, use the **sa-filter** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

sa-filter {**in** | **out**} {**list** *access-list-name* | **rp-list** *access-list-name*}
no sa-filter {**in** | **out**} {**list** *access-list-name* | **rp-list** *access-list-name*}

Syntax Description

in | **out**	Specifies incoming or outgoing SA filtering.
list *access-list-name*	Specifies an IP access list number or name. If no access list is specified, no (S, G) pairs from the peer are filtered.
rp-list *access-list-name*	Specifies an originating rendezvous point (RP) access list in SA messages.

Command Default

If the **sa-filter** command is not configured, no incoming or outgoing messages are filtered; all incoming SA messages are accepted from the peer, and all outgoing SA messages received are forwarded to the peer.

Command Modes

MSDP configuration

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Note You can configure the **sa-filter** command globally for MSDP (and is inheritable by MSDP peers); however, this global configuration can be overridden if it is issued again in peer configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

In the following example, only (S, G) pairs that pass access list 10 are forwarded in an SA message to the peer with IP address 131.107.5.4:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 131.107.5.4
RP/0/(config-msdp-peer)# sa-filter out list_10
```

In the following example, only (S, G) pairs for the rendezvous point that passes access list 151 are forwarded in an SA message to the peer with the IP address 131.107.5.4:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 131.107.5.4
RP/0/(config-msdp-peer)# sa-filter out rp-list list_151
```

Note The source and destination fields in the access list matches on the (S,G) fields in the SA messages. We recommend that the first address and mask field in the access list is used for the source and the second field in the access list is used for the group or destination.

Related Commands

Command	Description
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.

show msdp globals

To display the Multicast Source Discovery Protocol (MSDP) global variables, use the **show msdp globals** command in EXEC mode.

show msdp [ipv4] globals

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Some global variables associated with MSDP sessions are displayed, such as the originator ID, default peer, and connection state with Protocol Independent Multicast (PIM), Source.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show msdp globals** command:

```
RP/0/# show msdp globals

Multicast Source Discovery Protocol - msdp[405672]
  AS: 10, caching, originator: not set, default peer: not set
  Connected to PIM: yes
  Active RP              Grange/len     Source Count
                            ADV/RPF     (Total, Active)
  10.10.2.1             224.0.0.0/4      0,0
  10.10.10.3                0.0.0.0      1,1

  Max/active group count:     1/1
  Max/active SA count:     1/1

  General stats
  Current lists alloced/free:           2/0
  Total list items alloced/free:        9/1
  Total source buffers alloced/free:    1/0
  Total group buffers alloced/free:     1/0
  Total RP buffers alloced/free:        2/0
  TLV buffers alloced/free:             1/1
```

This table describes the significant fields shown in the display.

Table 7: show msdp globals Field Descriptions

Field	Description
AS	Local autonomous system.
caching	SA caching that is enabled.
originator	Local rendezvous point (RP).
default peer	Default peer to accept Source Active (SA) messages from when all Reverse Path Forwarding (RPF) rules fail.
Active RP	All RPs involved in sending SA messages to this router.
Grange/len	Multicast Group Range or Multicast Group Mask. The field is visible only when there is a specified group range for the local RP. If a group range is unspecified (for example, for RPs that advertise SAs) only the Advertiser address and the RPF information is displayed (see ADV/RPF below).
Source Count	Total and active SA messages advertised by the respective RP.
ADV/RPF	Advertiser and RPF entry.
Max/active group count	Maximum group count since router was booted and number of active groups.
Max/active SA count	Maximum SA message count since router was booted, and number of active SA messages.
Total source buffers alloced/free	Number of internal source buffers allocated and freed after allocation.
Total group buffers alloced/free	Number of internal group buffers allocated and freed after allocation.
Total RP buffers alloced/free	Number of internal RP buffers allocated and freed after allocation.
TLV buffers alloced/free	Number of internal time-to-live buffers allocated and freed after allocation.

Related Commands

Command	Description
show msdp peer, on page 77	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
show msdp sa-cache, on page 81	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

show msdp nsr

To display nonstop routing (NSR) information in the Multicast Source Discovery Protocol (MSDP), use the **show mrib nsr** command in the appropriate mode.

show msdp ipv4| ipv6 nsr

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show msdp nsr** command displays the current multicast NSR state for the MSDP. The state may be normal or activated for NSR. The activated state indicates that recovery is in progress due to a failure in MRIB or Protocol Independent Multicast (PIM). The total NSR timeout and time remaining are displayed until NSR expiration.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show msdp nsr** command:

```
RP/0/# show msdp nsr
```

Related Commands

Command	Description
show mrib nsr	Displays the state of NSR operation in the MRIB.
show igmp nsr	Displays the state of NSR operation for IGMP.
show pim nsr	Displays the state of NSR operation for PIM.

show msdp peer

To display information about the Multicast Source Discovery Protocol (MSDP) peer, use the **show msdp peer** command in EXEC mode.

show msdp [**ipv4**] **peer** [*peer-address*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
peer-address	(Optional) IP address or hostname of the MSDP peer for which information is displayed.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show msdp peer** command:

```
RP/0/# show msdp peer 10.10.10.2

MSDP Peer 10.10.10.2 (?), AS 20
Description:
 Connection status:
  State: Up, Resets: 0, Connection Source: 10.10.10.12
  Uptime(Downtime): 00:00:26, SA messages received: 0
  TLV messages sent/received: 1/1
 Output messages discarded: 0
  Connection and counters cleared 00:00:26 ago
 SA Filtering:
  Input (S,G) filter: none
  Input RP filter: none
  Output (S,G) filter: none
  Output RP filter: none
 SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: disabled
 Password: None
 Peer ttl threshold: 0
 Input queue size: 0, Output queue size: 0
```

This table describes the significant fields shown in the display.

Table 8: show msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the peer belongs.
State	State of the peer.
Uptime(Downtime)	Days and hours the peer is up or down, per state shown in previous column. If less than 24 hours, it is shown in terms of hours:minutes:seconds.
Msgs Sent/Received	Number of Source-Active (SA) messages sent to peer/number of SA messages received from peer.
Peer Name	Name of peer.
TCP connection source	Interface used to obtain IP address for TCP local connection address.
SA input filter	Name of the access list filtering SA input (if any).
SA output filter	Name of the access list filtering SA output (if any).
SA-Request filter	Name of the access list filtering SA request messages (if any).
Sending SA-Requests to peer	There are no peers configured to send SA request messages to.
Password	Information on the password. If the password is set on an active peer, “Configured, set on active socket” is displayed.
Peer ttl threshold	Multicast packets with an IP header that shows time-to-live greater than or equal to this value are sent to the MSDP peer.

Related Commands

Command	Description
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.
show msdp sa-cache, on page 81	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

show msdp rpf

To display the Multicast Source Discovery Protocol (MSDP) Reverse Path Forwarding (RPF) rule that governs whether an Source-Active (SA) from an originating RP will be accepted, use the **show msdp rpf** command in EXEC mode.

show msdp [**ipv4**] **rpf** *rpf-address*

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
rpf-address	IP address or hostname of the RPF next hop.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show msdp rpf** command displays the peer interface and autonomous system to which the SAs are sent and forwarded based on the MSDP RPF rule. The rule is displayed and applied on the RP address field of the arriving SAs.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show msdp rpf** command for RP peer 10.1.1.1:

```
RP/0/# show msdp rpf 10.1.1.1

RP peer for 172.16.1.1 is 10.1.1.1 AS 200, rule: 1
bgp/rib lookup: nexthop: 10.1.1.1, asnum: 200
```

This table describes the significant fields shown in the display.

Table 9: show msdp rpf Field Descriptions

Field	Description
RP peer for 172.16.1.1 is 10.1.1.1	IP address of the MSDP RPF peer.
AS 200	Autonomous system to which the peer belongs.
rule: 1	MSDP RPF rule that matches what was learned from SAs.
bgp/rib lookup:	Multicast RPF routing table lookup.

Field	Description
nexthop: 10.1.1.1	Router where the SA is sent to reach the final destination.
asnum: 200	Autonomous system number for the next-hop neighbor router.

show msdp sa-cache

To display the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers, use the **show msdp sa-cache** command in EXEC mode.

show msdp [**ipv4**] **sa-cache** [*source-address*] [*group-address*] [**all**] [**asnum** *as-number*] [**peer** *peer-address*] [**rpaddr** *rp-address*] [**summary**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
source-address	(Optional) Source address or hostname of the source about which (S, G) information is displayed.
group-address	(Optional) Group address or name of the group about which (S, G) information is displayed.
all	(Optional) Displays all Source Active (SA) entries with PI (PIM Interested) flags.
asnum *as-number*	(Optional) Displays SA entries of the specified autonomous system number. Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.
peer *peer-address*	(Optional) Displays peer entry information, including peer name and peer address.
rpaddr *rp-address*	(Optional) Displays SA entries that match the specified rendezvous point (RP) address.
summary	(Optional) Displays the count of all SA entries, RPs, sources, and groups.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show msdp sa-cache** command is used to examine the (S, G) entries and the attributes, flags (L, E, EA), uptime, autonomous system number, and RP addresses that are stored in the SA cache.

These guidelines apply when this command is used:

- The **cache-sa-state** command is enabled by default.
- When you specify the **summary** keyword, the total number of cache, group, and source entries, and entries advertised by each RP and autonomous system are displayed.
- When you specify two addresses or names, an (S, G) entry corresponding to those addresses is displayed.
- When you specify a single group address, all sources for that group are displayed.
- When you specify no options, the entire SA cache is displayed, excluding the PI flag entries.

Task ID

Task ID	Operations
multicast	read

Examples

This is a sample output from the **show msdp sa-cache** command:

```
RP/0/# show msdp sa-cache

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.
Cache Entry:
(10.10.5.102, 239.1.1.1), RP 10.10.4.3, AS 20, 15:44:03/00:01:17
Learned from peer 10.10.2.2, RPF peer 10.10.2.2
SA's recvd 1049, Encapsulated data received: 0
grp flags: PI, src flags: E, EA, PI
```

This table describes the significant fields shown in the display.

Table 10: show msdp sa-cache Field Descriptions

Field	Description
(10.10.5.102, 239.1.1.1)	The first address (source) is sending to the second address (group).
RP 10.10.4.3	Rendezvous point (RP) address in the originating domain where the SA messages started.
MBGP/AS 20	RP is in autonomous system AS 20 according to the unicast RPF table: • If Multiprotocol Border Gateway Protocol (MBGP) is not configured—RIB table 1. • If MBGP is configured—RIB table 2 or multicast table.
15:44:03/00:01:17	The route has been cached for 15 hours, 44 minutes, and 3 seconds. If no SA message is received in 1 minute and 17 seconds, the route is removed from the SA cache.
Encapsulated data received: 0	MSDP SA captures any data information when the source starts so that the receiver does not miss data when the SA path is established.

The following is sample output using the **all** keyword option:

```
RP/0/# show msdp sa-cache all

MSDP Flags:
E - set MRIB E flag , L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.  Timers age/expiration,
Cache Entry:

(*, 239.1.1.1), RP 0.0.0.0, AS 0, 06:32:18/expired
Learned from peer local, RPF peer local
SAs recvd 0, Encapsulated data received: 0 grp flags: PI,  src flags:
```

This table describes the significant fields shown in the display.

Table 11: show msdp sa-cache all Field Descriptions

Field	Description
(*, 239.1.1.1)	Protocol Independent Multicast (PIM) interest in the group due to a local Internet Group Management Protocol (IGMP) join.
RP 0.0.0.0	There is no RP associated with this entry.
AS 0	This entry is 0, autonomous system (AS) rendezvous point (RP) is null.
06:32:18/expired	Route is alive in hours, minutes, and seconds. Note that MSDP does not monitor this route as it is received from the MRIB and PIM.

The following is sample output using the **summary** keyword option:

```
RP/0/# show msdp sa-cache summary

Total # of SAs = 3
Total # of RPs = 2
Total # of Sources = 1
Total # of Groups = 3

Originator-RP   SA total   RPF peer

172.16.1.1         0          0.0.0.0
172.17.1.1         3          172.17.1.1

AS-num  SA total

200     3
```

This table describes the significant fields shown in the display.

Table 12: show msdp sa-cache summary Field Descriptions

Field	Description
Total # of SAs	Total number of SAs that are currently active in the system.
Total # of RPs	Total number of RPs that have distributed the SA information to this system.
Total # of Sources	Total number of sources that are active from all domains.
Total # of Groups	Total number of groups to which sources are sending data from all domains.
Originator-RP	SA information based on the individual RPs and the originating domains that distributed them.
AS-num	SA information based on the originating autonomous system.

The following is sample output using the **asnum** keyword option:

```
RP/0/# show msdp sa-cache asnum 200
```

```
MSDP Flags:
E - set MRIB E flag , L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.  Timers age/expiration,
Cache Entry:

(172.31.1.1, 239.1.1.1), RP 5.1.1.1, AS 200, 00:00:25/00:02:04
  Learned from peer 5.1.1.1, RPF peer 172.17.1.1
  SAs recvd 1, Encapsulated data received: 100
    grp flags: none,  src flags: EA
(172.31.1.1, 239.1.1.2), RP 172.17.1.1, AS 200, 00:00:16/00:02:13
  Learned from peer 172.17.1.1, RPF peer 172.17.1.1
  SAs recvd 1, Encapsulated data received: 100
    grp flags: none,  src flags: EA
(172.31.1.1, 239.1.1.3), RP 172.17.1.1, AS 200, 00:00:13/00:02:16
  Learned from peer 172.17.1.1, RPF peer 172.17.1.1
  SAs recvd 1, Encapsulated data received: 100
    grp flags: none,  src flags: EA
```

Related Commands

Command	Description
cache-sa-state, on page 52	Controls cache source-active (SA) state on a router.
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.

show msdp statistics peer

To display Multicast Source Discovery Protocol (MSDP) peer statistic counters, use the **show msdp statistics peer** command in EXEC mode

.

show msdp [**ipv4**] **statistics peer** [*peer-address*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
peer-address	(Optional) IP address or name of the MSDP peer.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show msdp statistics peer** command displays MSDP peer statistics such as the number of keepalive messages sent and received and the number of Source-Active (SA) entries sent and received.

If you do not specify an MSDP peer with the *peer-address* argument, this command displays statistics for all MSDP peers.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show msdp statistics peer** command:

```
RP/0/# show msdp statistics peer

MSDP Peer Statistics :-

Peer 10.1.2.3 : AS is 10, State is Up, 0 active SAs
    TLV Rcvd : 57 total
               57 keepalives, 0 notifications
               0 SAs, 0 SA Requests
               0 SA responses, 0 unknowns
    TLV Sent : 57 total
               54 keepalives, 0 notifications
               3 SAs, 0 SA Requests
               0 SA responses
    SA msgs  : 0 received, 3 sent
Peer 10.2.3.4 : AS is 0, State is Connect, 0 active SAs
    TLV Rcvd : 0 total
               0 keepalives, 0 notifications
               0 SAs, 0 SA Requests
               0 SA responses, 0 unknowns
```

```
TLV Sent : 0 total
           0 keepalives, 0 notifications
           0 SAs, 0 SA Requests
           0 SA responses
SA msgs  : 0 received, 0 sent
```

This table describes the significant fields shown in the display.

Table 13: show msdp statistic peer Field Descriptions

Field	Description
Peer 10.1.2.3	All statistics are displayed for MSDP peer.
AS 10	Peer belongs to autonomous system (AS) 10.
State is UP	Peer state is established.
0 active SAs	There are no active SAs from this peer.
TLV Rcvd	Information about the time-to-lives (TLVs) received from this peer.
TLV Sent	Information about the TLVS sent to this peer.
SA msgs	Information about the SA messages for this peer.

Related Commands

Command	Description
clear msdp stats, on page 57	Resets Multicast Source Discovery Protocol (MSDP) peer statistic counters.

show msdp summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the **show msdp summary** command in EXEC mode.

show msdp [**ipv4**] **summary**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show msdp summary** command displays peer status such as the following:

- Peer address
- Peer autonomous system
- Peer state
- Uptime and downtime
- Number of Source-Active (SA) messages sent or received

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show msdp summary** command:

```
RP/0/# show msdp summary

Out of Resource Handling Enabled
Maximum External SA's Global : 20000
Current External Active SAs : 0

MSDP Peer Status Summary
Peer Address       AS    State     Uptime/   Reset  Peer    Active Cfg.Max    TLV
                                   Downtime  Count  Name    SA Cnt Ext.SAs   recv/sent
10.1.1.1           0     NoIntf    00:10:07  0      ?       0      0           0/0
```

This table describes the significant fields shown in the display.

Table 14: show msdp summary Field Descriptions

Field	Description
Peer Address	Neighbor router address from which this router has MSDP peering established.
AS	Autonomous system to which this peer belongs.
State	State of peering, such as UP, inactive, connect, and NoIntf.
Uptime/Downtime	MSDP peering uptime and downtime in hours, minutes, and seconds.
Reset Count	Number of times the MSDP peer has reset.
Peer Name	DNS name of peer (if available).
Active SA Cnt	Total number of SAs that are active on this router.
Cfg. Max Ext. SAs	Total number of maximum external SAs after the SAs are dropped. If 0, nothing is configured.
TLV recv/sent	Total number of time-to-lives (TLVs) sent and received.

Related Commands

Command	Description
show msdp peer, on page 77	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
show msdp sa-cache, on page 81	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

shutdown (MSDP)

To shut down a Multicast Source Discovery Protocol (MSDP) peer, use the **shutdown** command in peer configuration mode. To return to the default behavior, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **shutdown** command to shut down the peer. To configure many MSDP commands for the same peer, shut down the peer, configure it, and activate the peer later.

You might also want to shut down an MSDP session without losing configuration information for the peer.

When a peer is shut down, the TCP connection is terminated and is not restarted.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to shut down the peer with the address 172.16.5.4:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# peer 172.16.5.4
RP/0/(config-msdp-peer)# shutdown
```

Related Commands

Command	Description
show msdp peer, on page 77	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.

show msdp vrf context

To show the MSDP information configured for a VPN routing and forwarding (VRF) context, use the **show msdp vrf context** command in EXEC mode.

show msdp vrf *vrf-name* **context**

Syntax Description

vrf-name	VPN routing and forwarding (VRF) interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read

Example

This example shows how to use the **show msdp vrf context** command:

```
RP/0/ # show msdp vrf red context
Fri Feb  8 18:13:51.599 PST

MSDP context information for red
  VRF ID                     : 0x60000002
  Table ID                   : 0xe0000002
  Table Count (Active/Total) : 1/1
Inheritable Configuration
  TTL                 : 2
  Maximum SAs         : 0
  Keepalive Period    : 30
  Peer Timeout Period : 75
  Connect Source      :
  SA Filter In        :
  SA Filter Out       :
  RP Filter In        :
  RP Filter Out       :
Configuration
  Originator Address         : 0.0.0.0
  Originator Interface Name  :
  Default Peer Address       : 0.0.0.0
  SA Holdtime                : 150
  Allow Encaps Count         : 0
  Context Maximum SAs        : 20000
SA Cache Counts    (Current/High Water Mark)
```

```
  Groups       :          0/0
  Sources      :          0/0
  RPs          :          2/0
  External SAs :          0/0
MRIB Update Counts
  Total updates        : 2
  With no changes      : 0
  (*,G) routes         : 2
  (S,G) routes         : 0
MRIB Update Drops
  Invalid group        : 0
  Invalid group length : 0
  Invalid source       : 0
  Auto-RP Address      : 2
```

ttl-threshold (MSDP)

To limit which multicast data packets are sent in Source-Active (SA) messages to a Multicast Source Discovery Protocol (MSDP) peer, use the **ttl-threshold** command in MSDP configuration mode or peer configuration mode. To return to the default behavior, use the **no** form of this command.

ttl-threshold *ttl*
no ttl-threshold *ttl*

Syntax Description

ttl	Time to live value. Range is 1 to 255.

Command Default

ttl : 1

Command Modes

MSDP configuration

MSDP peer configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ttl-threshold** command limits which multicast data packets are sent in data-encapsulated Source-Active (SA) messages. Only multicast packets with an IP header time-to-live (TTL) greater than or equal to the *ttl* argument are sent to the MSDP peer specified by the IP address or name.

Use the **ttl-threshold** command to use TTL to examine your multicast data traffic. For example, you can limit internal traffic to a TTL of 8. If you want other groups to go to external locations, send the packets with a TTL greater than 8.

Note This command can be configured globally for MSDP (and to be inheritable by MSDP peers). However this global configuration can be overridden if issued again in peer configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure a TTL threshold of eight hops:

```
RP/0/(config)# router msdp
RP/0/(config-msdp)# ttl-threshold 8
```

Related Commands

Command	Description
peer (MSDP), on page 70	Configures a Multicast Source Discovery Protocol (MSDP) peer.



Multicast PIM Commands

- accept-register, on page 95
- auto-rp candidate-rp, on page 96
- bsr candidate-bsr, on page 98
- bsr candidate-rp, on page 100
- clear pim counters, on page 102
- clear pim topology, on page 105
- dr-priority, on page 107
- global maximum, on page 108
- global maximum bsr crp-cache threshold, on page 109
- global maximum group-mappings bsr threshold, on page 111
- hello-interval (PIM), on page 113
- interface (PIM), on page 115
- join-prune-interval, on page 117
- join-prune-mtu, on page 118
- maximum register-states, on page 119
- maximum route-interfaces, on page 120
- maximum routes, on page 121
- mofrr, on page 122
- neighbor-check-on-recv enable, on page 124
- neighbor-check-on-send enable , on page 125
- neighbor-filter, on page 126
- nsf lifetime (PIM), on page 127
- old-register-checksum, on page 128
- router pim, on page 129
- rp-address, on page 130
- rpf topology route-policy, on page 132
- rpf-redirect, on page 133
- rpf-redirect bundle, on page 134
- rp-static-deny , on page 136
- rpf-vector , on page 137
- rpf-vector use-standard-encoding , on page 138
- show auto-rp candidate-rp, on page 139
- show pim global summary, on page 141

- show pim nsr, on page 143
- show pim rpf-redirect, on page 145
- show pim rpf-redirect route, on page 146
- show pim segment-database, on page 147
- show pim context, on page 149
- show pim context table, on page 152
- show pim group-map, on page 154
- show pim interface, on page 156
- show pim join-prune statistic, on page 159
- show pim mstatic, on page 161
- show pim neighbor, on page 163
- show pim nsf, on page 166
- show pim range-list, on page 168
- show pim rpf, on page 170
- show pim rpf hash, on page 172
- show pim rpf route-policy statistics, on page 174
- show pim rpf route-policy test, on page 176
- show pim rpf summary, on page 178
- show pim summary, on page 180
- show pim topology, on page 182
- show pim topology detail, on page 188
- show pim topology entry-flag, on page 191
- show pim topology interface-flag, on page 193
- show pim topology summary, on page 195
- show pim traffic, on page 197
- show pim tunnel info, on page 199
- show pim vrf vrf_name rpf, on page 201
- show pim vrf vrf_name topology, on page 202
- spt-threshold infinity, on page 203
- ssm, on page 204

accept-register

To configure a rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the **accept-register** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

accept-register *access-list-name*
no accept-register

Syntax Description

access-list-name	Access list number or name.

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **accept-register** command prevents unauthorized sources from registering with the rendezvous point. If an unauthorized source sends a register message to the rendezvous point, the rendezvous point immediately sends back a register-stop message.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to restrict the rendezvous point. Sources in the Source Specific Multicast (SSM) range of addresses are not allowed to register with the rendezvous point. These statements need to be configured only on the rendezvous point.

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# accept-register no-ssm-range
RP/0/(config-pim-default-ipv4)# exit
RP/0/(config)# ipv4 access-list no-ssm-range
RP/0/(config-ipv4-acl)# deny ipv4 any 232.0.0.0 0.255.255.255
RP/0/(config-ipv4-acl)# permit any
```

auto-rp candidate-rp

To configure a router as a Protocol Independent Multicast (PIM) rendezvous point (RP) candidate that sends messages to the well-known CISCO-RP-ANNOUNCE multicast group (224.0.1.39), use the **auto-rp candidate-rp** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

auto-rp candidate-rp *type interface-path-id* **scope** *ttl-value* [**group-list** *access-list-name*] [**interval** *seconds*] [**bidir**]
no auto-rp candidate-rp *type interface-path-id* **scope** *ttl-value* [**group-list** *access-list-name*] [**interval** *seconds*] [**bidir**]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
scope *ttl-value*	Specifies a time-to-live (TTL) value (in router hops) that limits the scope of the auto-rendezvous point (Auto-RP) announce messages that are sent out of that interface. Range is 1 to 255.
group-list *access-list-name*	(Optional) Specifies an access list that describes the group ranges for which this router is the rendezvous point.
interval *seconds*	(Optional) Specifies the time between rendezvous point announcements. Range is 1 to 600.
bidir	(Optional) Specifies a bidirectional rendezvous point for PIM.

Command Default

A router is not configured as a PIM rendezvous point candidate by default.

seconds : 60

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **auto-rp candidate-rp** command is used by the rendezvous point for a multicast group range. The router sends an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate rendezvous point for the groups in the range described by the access list.

When the **interval** keyword is specified, the interval between Auto-RP announcements is set to number of *seconds* with the total hold time of the announcements automatically set to three times the interval time. The recommended interval time range is from 1 to 180 seconds.

The hold time of the Auto-RP announcement is the time for which the announcement is valid. After the designated hold time, the announcement expires and the entry is purged from the mapping cache until there is another announcement.

If the optional **group-list** keyword is omitted, the group range advertised is 224.0.0.0/4. This range corresponds to all IP multicast group addresses, which indicates that the router is willing to serve as the rendezvous point for all groups.

A router may be configured to serve as a candidate rendezvous point for more than one group range by a carefully crafted access list in the router configuration.



Note The **auto-rp candidate-rp** command is available for IPv4 address prefixes only.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to send rendezvous point announcements from all PIM-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as a rendezvous point is the IP address associated with GigabitEthernet interface 0/1/0/1. Access list 5 designates the groups that this router serves as the rendezvous point.

```
Router(config)# ipv4 access-list 5
Router(config-ipv4-acl)# permit ipv4 any 224.0.0.0 15.255.255.255
Router(config-ipv4-acl)# exit
Router(config)# router pim
Router(config-pim-default-ipv4)# auto-rp candidate-rp HundredGigE 0/0/0/24 scope 31
group-list 5
Router(config-pim-default-ipv4)# end
```

The router identified in the following example advertises itself as the candidate rendezvous point and is associated with loopback interface 0 for the group ranges 239.254.0.0 to 239.255.255.255 and 224.0.0.0 to 231.255.255.255:

```
Router(config)# ipv4 access-list 10
Router(config-ipv4-acl)# permit ipv4 any 239.254.0.0 0.0.255.255
Router(config-ipv4-acl)# exit
Router(config)# router pim
Router(config-pim-default-ipv4)# auto-rp candidate-rp loopback 0 scope 16 group-list 10
Router(config-pim-default-ipv4)# end
```

bsr candidate-bsr

To configure the router to announce its candidacy as a bootstrap router (BSR), use the **bsr candidate-bsr** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

bsr candidate-bsr *ip-address* [**hash-mask-len** *length*] [**priority** *value*]
no bsr candidate-bsr

Syntax Description

ip-address	IP address of the BSR router for the domain. For IPv4, this is an IP address in four-part dotted-decimal notation. For IPv6, the IP address is specified in hexadecimal format using 16-bit values between colons.
hash-mask-len *length*	(Optional) Specifies the length of a mask that is to be used in the hash function. • All groups with the same seed hash (correspond) to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups. • For IPv4 addresses, we recommend a value of 30. The range is 0 to 32. • For IPv6 addresses, we recommend a value of 126. The range is 0 to 128.
priority *value*	(Optional) Specifies the priority of the candidate BSR. Range is 1 to 255. We recommend the BSR with the higher priority. If the priority values are the same, the router with the higher IP address is the BSR.

Command Default

- *value* : 1
- Default C-RP cache state limit in both Candidate BSR and Elected BSR is 100.
- Configurable maximum C-RP cache in both BSR and Elected BSR is in the range of 1 - 100000.
- Default RP-group mapping state limit in PIMv2 router is 100.
- Configurable maximum RP-group mapping state in PIMv2 router is in the range of 1 - 100000.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **bsr candidate-bsr** command causes the router to send bootstrap messages to all its Protocol Independent Multicast (PIM) neighbors, with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, the PIM neighbor caches the current address and forwards the bootstrap message. Otherwise, the bootstrap message is dropped.

This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Note Use the **bsr candidate-bsr** command only in backbone routers with good connectivity to all parts of the PIM domain. A subrouter that relies on an on-demand dial-up link to connect to the rest of the PIM domain is not a good candidate BSR.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router as a candidate BSR with a hash mask length of 30:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# bsr candidate-bsr 10.0.0.1 hash-mask-len 30
```

bsr candidate-rp

To configure the router to advertise itself as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP) to the bootstrap router (BSR), use the **bsr candidate-rp** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

bsr candidate-rp *ip-address* [**group-list** *access-list*] [**interval** *seconds*] [**priority** *value*]**[bidir]**
no bsr candidate-rp *ip-address*
[bidir]

Syntax Description

ip-address	IP address of the router that is advertised as a candidate rendezvous point address.
group-list *access-list*	(Optional) Specifies the IP access list number or name that defines the group prefixes that are advertised in association with the rendezvous point address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Specifies the candidate rendezvous point advertisement interval in seconds. Range is 30 to 600.
priority *value*	(Optional) Indicates the rendezvous point priority value. Range is 1 to 255.
bidir	(Optional) Configures a bidirectional (bidir) rendezvous point.

Command Default

- *value* : 1
- Default C-RP cache state limit in both Candidate BSR and Elected BSR is 100.
- Configurable maximum C-RP cache in both BSR and Elected BSR is in the range of 1 - 100000.
- Default RP-group mapping state limit in PIMv2 router is 100.
- Configurable maximum RP-group mapping state in PIMv2 router is in the range of 1 - 100000.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **bsr candidate-rp** command causes the router to send a PIM Version 2 message advertising itself as a candidate rendezvous point to the BSR. The addresses allowed by the access list, together with the router identified by the IP address, constitute the rendezvous point and its range of addresses for which it is responsible.



Note Use the **bsr candidate-rp** command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dial-up link to connect to the rest of the PIM domain is not a good candidate rendezvous point.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router to advertise itself as a candidate rendezvous point to the BSR in its PIM domain. Access list number 4 specifies the group prefix associated with the candidate rendezvous point address 172.16.0.0. This rendezvous point is responsible for the groups with the prefix 239.

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# bsr candidate-rp 172.16.0.0 group-list 4
RP/0/(config-pim-default-ipv4)# exit
RP/0/(config)# ipv4 access-list 4
RP/0/(config-ipv4-acl)# permit ipv4 any 239.0.0.0 0.255.255.255
RP/0/(config-ipv4-acl)# end
```

Related Commands

Command	Description
bsr candidate-bsr, on page 98	Configures the router to announce its candidacy as a bootstrap router (BSR).

clear pim counters

To clear Protocol Independent Multicast (PIM) counters and statistics, use the **clear pim counters** command in EXEC mode.

clear pim [**vrf** *vrf-name*] [**ipv4**] **counters**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not explicitly specify a particular VRF, the default VRF is used.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows sample output before and after clearing PIM counters and statistics:

```
RP/0/# show pim traffic
PIM Traffic Counters
Elapsed time since counters cleared: 1d01h

                  Received                       Sent
Valid PIM Packets 15759217                    15214426
Hello                9207                       12336
Join-Prune         1076805                      531981
Data Register     14673205                           0
Null Register        73205                           0
Register Stop            0                    14673205
Assert                   0                           0
Batched Assert           0                           0
Bidir DF Election        0                           0
BSR Message              0                           0
Candidate-RP Adv.        0                           0

Join groups sent                                     0
Prune groups sent                                    0
Output JP bytes                                      0
Output hello bytes                                4104

Errors:
```

```
Malformed Packets                                  0
Bad Checksums                                      0
Socket Errors                                      0
Subnet Errors                                      0
Packets dropped since send queue was full          0
Packets dropped due to invalid socket              0
Packets which couldn't be accessed                 0
Packets sent on Loopback Errors                    6
Packets received on PIM-disabled Interface         0
Packets received with Unknown PIM Version          0
```

This table describes the significant fields shown in the display.

Table 15: show pim traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Time (in days and hours) that had elapsed since the counters were cleared with the **clear pim counters** command.
Valid PIM Packets	Total PIM packets that were received and sent.
HelloJoin-PruneRegisterRegister StopAssert Bidir DF Election	Specific type of PIM packets that were received and sent.
Malformed Packets	Invalid packets due to format errors that were received and sent.
Bad Checksums	Packets received or sent due to invalid checksums.
Socket Errors	Packets received or sent due to errors from the router's IP host stack sockets.
Packets dropped due to invalid socket	Packets received or sent due to invalid sockets in the router's IP host stack.
Packets which couldn't be accessed	Packets received or sent due to errors when accessing packet memory.
Packets sent on Loopback Errors	Packets received or sent due to use of loopback interfaces.
Packets received on PIM-disabled Interface	Packets received or sent due to use of interfaces not enabled for PIM.
Packets received with Unknown PIM Version	Packets received or sent due to invalid PIM version numbers in the packet header.

```
RP/0/# clear pim counters
RP/0/# show pim traffic


PIM Traffic Counters
Elapsed time since counters cleared: 00:00:04

BSR Message                                    0   0
Candidate-RP Adv.                              0   0

Join groups sent                                   0
Prune groups sent                                  0
```

```
Output JP bytes                                    0
Output hello bytes                                 0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Socket Errors                                      0
Subnet Errors                                      0
Packets dropped since send queue was full          0
Packets dropped due to invalid socket              0
Packets which couldn't be accessed                 0
Packets sent on Loopback Errors                    0
Packets received on PIM-disabled Interface         0
Packets received with Unknown PIM Version          0
```

Related Commands

Command	Description
show pim traffic, on page 197	Displays Protocol Independent Multicast (PIM) traffic counter information.

clear pim topology

To clear group entries from the Protocol Independent Multicast (PIM) topology table and reset the Multicast Routing Information Base (MRIB) connection, use the **clear pim topology** command in EXEC mode.

clear pim [**vrf** *vrf-name*] [**ipv4**] **topology** [*ip-address-name* | **reset**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ip-address-name	(Optional) Can be either one of the following: • Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the **domain IPv4** or **domain IPv6 host** command. • IP address of the multicast group, in IPv4 or IPv6 format according to the specified address family.
reset	(Optional) Deletes all entries from the topology table and resets the MRIB connection.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **clear pim topology** command clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as Internet Group Management Protocol (IGMP) local membership, is retained. If a multicast group is specified, only those group entries are cleared.

When the command is used with no arguments, all group entries located in the PIM topology table are cleared of PIM protocol information.

If the **reset** keyword is specified, all information from the topology table is cleared and the MRIB connections are automatically reset. This form of the command can be used to synchronize state between the PIM topology table and the MRIB database. The **reset** keyword should be strictly reserved to force synchronized PIM and MRIB entries when communication between the two components is malfunctioning.

If you do not explicitly specify a particular VRF, the default VRF is used.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to clear the PIM topology table:

```
RP/0/# clear pim topology
```

dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **dr-priority** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

dr-priority *value*
no dr-priority

Syntax Description

value	An integer value to represent DR priority. Range is from 0 to 4294967295.

Command Default

If this command is not specified in interface configuration mode, the interface adopts the DR priority value specified in PIM configuration mode.

If this command is not specified in PIM configuration mode, the DR priority value is 1.

Command Modes

PIM interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If all the routers on the LAN support the DR priority option in the PIM Version 2 (PIMv2) hello message that they send, you can force the DR election by use of the **dr-priority** command so that a specific router on the subnet is elected as DR. The router with the highest DR priority becomes the DR.

When PIMv2 routers receive a hello message without the DR priority option (or when the message has priority of 0), the receiver knows that the sender of the hello message does not support DR priority and that DR election on the LAN segment should be based on IP address alone.

Note If this command is configured in PIM configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from PIM interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the router to use DR priority 4 for Packet-over-SONET/SDH (POS) interface 0/1/0/0, but other interfaces will inherit DR priority 2:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# dr-priority 2
RP/0/(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/(config-pim-ipv4-if)# dr-priority 4
```

global maximum

To configure the global maximum limit states that are allowed by Protocol Independent Multicast (PIM) for all VRFs, use the **global maximum** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

global maximum [**register states** | **route-interfaces** | **routes** *number*]
no global maximum [**register states** | **route-interfaces** | **routes**]

Syntax Description

register states	(Optional) Specifies the PIM source register states for all VRFs. Range is 0 to 75000. **Note** PIM registers throttle at 20000 due to the default global threshold set.
route-interfaces	(Optional) Specifies the total number of PIM interfaces on routes for all VRFs. Range is 1 to 600000.
routes	(Optional) Specifies the PIM routes for all VRFs. Range is 1 to 200000.

Command Default

Default value is 20000.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **global maximum** command is used to set an upper limit for register states, route interfaces, and routes on all VRFs. When the limit is reached, PIM discontinues route interface creation for its topology table.

Note After the maximum threshold values for routes or route-interfaces are reached, throttling begins and will remain in effect until the values fall below 95% of the Maximum value.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the upper limit for PIM route interfaces on all VRFs to 200000:

```
RP/0/# router pim
RP/0/(config-pim-default-ipv4)# global maximum route-interfaces 200000
```

global maximum bsr crp-cache threshold

To configure the global maximum bsr crp-cache threshold limit that are allowed by Protocol Independent Multicast (PIM) for all VRFs, use the **global maximum bsr** *crp-cache threshold* command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

[**global**] **maximum** [**bsr** *crp-cache threshold*]
no [**global**] **maximum** [**bsr** *crp-cache threshold*]

Syntax Description

global	(Optional) Configures the maximum value for CRP cache and threshold limit to the sum of the caches in all VRFs.
crp-cache	Specifies the CRP cache value. The range is from 1 to 10000.
threshold	Specifies the threshold value for the crp-cache value. Range is between 1 to the set crp-cache value.

Command Default

No default behavior or values.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **global maximum bsr** command is used to the threshold limits for the crp-cache levels.

Use the **global** keyword to configure the maximum value for CRP cache and threshold limit to the sum of the caches in all VRF. However, each VRF, including the default, will still have its own smaller maximum and threshold values. To set the maximum and threshold values in the default VRF, you should omit the **global** keyword.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set a crp-cache of 2000 and the threshold level to 500 for the crp-cache in the router PIM configuration mode.

```
RP/0/# router pim

RP/0/(config-pim)# global maximum bsr crp-cache 2000 ?
```

```
   threshold  Set threshold to print warning
   <cr>
RP/0/(config-pim)# global maximum bsr crp-cache 2000 threshold ?
   <1-2000>  Threshold value
RP/0/(config-pim)# global maximum bsr crp-cache 2000 threshold 500
RP/0/(config-pim)#
```

The following example shows how to set a crp-cache of 2000 and the threshold level to 500 for the crp-cache in the router PIM configuration mode in VRF sub-mode.

```
RP/0/# router pim

RP/0/(config-pim)# address-family ipv4

RP/0/(config-pim-default-ipv4)# global maximum bsr crp-cache 2000 threshold 500

RP/0/(config-pim-default-ipv4)# maximum bsr crp-cache 1800 threshold 450

RP/0/(config-pim-default-ipv4)#
```

The following configuration shows how to set the maximum and threshold level in the default VRF, while all VRFs together have a larger global maximum and threshold level:

```
RP/0/# router pim

RP/0/(config-pim)# address-family ipv4

RP/0/(config-pim-default-ipv4)# global maximum bsr crp-cache 600 threshold 550

RP/0/(config-pim-default-ipv4)# maximum bsr crp-cache 500 threshold 450

RP/0/(config-pim-default-ipv4)#
```

global maximum group-mappings bsr threshold

To configure the global maximum group-mappings and the threshold levels that are allowed by Protocol Independent Multicast (PIM) for all VRFs, use the **global maximum group-mappings** *bsr threshold* command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

global maximum [**group-mappings** *bsr threshold*]
no global maximum [**group-mappings** *bsr threshold*]

Syntax Description

bsr	Specifies the bsr value. Range is 1 to 10000.
threshold	Specifies the threshold value for the bsr value. Range is between 1 to the set bsr value.

Command Default

No default behavior or values.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **global maximum group-mappings** command is used to the threshold limits for the crp-cache levels.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set a bsr of 2000 and the threshold level to 500 for the bsr in the router PIM configuration mode.

```
RP/0/# router pim

RP/0/(config-pim)# global maximum group-mappings bsr

RP/0/(config-pim)# global maximum group-mappings bsr 2000 threshold ?
   <1-2000>  Threshold value
RP/0/(config-pim)# global maximum group-mappings bsr 2000 threshold 500
RP/0/(config-pim)#
```

The following example shows how to set a crp-cache of 2000 and the threshold level to 500 for the crp-cache in the router PIM configuration mode in VRF sub-mode.

```
RP/0/# router pim
RP/0/(config-pim)# address-family ipv4
```

```
RP/0/(config-pim-default-ipv4)# global maximum bsr-crp-cache 2000 threshold 500
RP/0/(config-pim-default-ipv4)# maximum bsr-crp-cache 1800 threshold 450
```

hello-interval (PIM)

To configure the frequency of Protocol Independent Multicast (PIM) hello messages, use the **hello-interval** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

hello-interval *seconds*
no hello-interval

Syntax Description

seconds	Interval at which PIM hello messages are sent. Range is 1 to 3600.

Command Default

Default is 30 seconds.

Command Modes

PIM interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Routers configured for IP multicast send PIM hello messages to establish PIM neighbor adjacencies and to determine which router is the designated router (DR) for each LAN segment (subnet).

To establish these adjacencies, at every hello period, a PIM multicast router multicasts a PIM router-query message to the All-PIM-Routers (224.0.0.13) multicast address on each of its multicast-enabled interfaces.

PIM hello messages contain a hold-time value that tells the receiver when the neighbor adjacency associated with the sender should expire if no further PIM hello messages are received. Typically the value of the hold-time field is 3.5 times the interval time value, or 120 seconds if the interval time is 30 seconds.

Use the **show pim neighbor** command to display PIM neighbor adjacencies and elected DRs.

Note If you configure the **hello-interval** command in PIM configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from PIM interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the PIM hello message interval to 45 seconds. This setting is adopted by all interfaces excluding the 60 second interval time set for Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# hello-interval 45
```

```
RP/0/(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/(config-pim-ipv4-if)# hello-interval 60
```

Related Commands

Command	Description
dr-priority, on page 107	Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.
show pim neighbor, on page 163	Displays the Protocol Independent Multicast (PIM) neighbors discovered by means of PIM hello messages.

interface (PIM)

To configure Protocol Independent Multicast (PIM) interface properties, use the **interface** command in PIM configuration mode. To disable multicast routing on an interface, use the **no** form of this command.

interface *type interface-path-id*
no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **interface** command to configure PIM routing properties for specific interfaces. Specifically, this command can be used to override the global settings for the following commands:

- dr-priority
- hello-interval
- join-prune-interval

Use the **interface** command also to enter PIM interface configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enter interface configuration mode to configure PIM routing properties for specific interfaces:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# interface pos 0/1/0/0
```

```
RP/0/
/CPU0:router(config-pim-ipv4-if)#
```

Related Commands

Command	Description
dr-priority, on page 107	Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.
hello-interval (PIM), on page 113	Configures the frequency of Protocol Independent Multicast (PIM) hello messages.
join-prune-interval, on page 117	Configures the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic.

join-prune-interval

To configure the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic, use the **join-prune-interval** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

join-prune-interval *seconds*
no join-prune-interval

Syntax Description

seconds	Interval, in seconds, at which PIM multicast traffic can join or be removed from the shortest path tree (SPT) or rendezvous point tree (RPT). Range is 10 to 600.

Command Default

If this command is not specified in PIM interface configuration mode, the interface adopts the join and prune interval parameter specified in PIM configuration mode.

If this command is not specified in PIM configuration mode, the join and prune interval is 60 seconds.

Command Modes

PIM interface configuration

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Note If this command is configured in PIM configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from PIM interface configuration mode.

The **join-prune-interval** command is used to configure the frequency at which a PIM sparse-mode router sends periodic join and prune messages.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to change the join and prune interval time to 90 seconds on Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/(config-pim-ipv4-if)# join-prune-interval 90
```

join-prune-mtu

To configure the maximum size of a PIM Join/Prune message, use the **join-prune-mtu** command in the appropriate mode. To return to the default value, use the **no** form of the command.

join-prune-mtu *value*
no join-prune-mtu *value*

Syntax Description

value	Join-prune MTU in bytes. Range is 576 to 65535.

Command Default

65535 bytes

Command Modes

Router PIM configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The actual maximum size used for PIM Join/Prune messages is the smaller of the, IP MTU value of the interface and the join-prune-mtu value. In normal operation without this configuration, the PIM Join/Prune packet is packed with Join/Prune messages until the interface MTU size limit is reached. This can lead to large PIM Join/Prune message packets getting sent out, which may affect the processing efficiency on some neighboring routers. Configuring the maximum size of a PIM Join/Prune message helps controlling the MTU size of the PIM Join/Prune packet getting sent out.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **join-prune mtu** command:

```
RP/0/ (config-pim) # join-prune-mtu 1000
```

maximum register-states

To configure the maximum number of sparse-mode source register states that is allowed by Protocol Independent Multicast (PIM), use the **maximum register-states** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

maximum register-states *number*
no maximum register-states

Syntax Description

number	Maximum number of PIM sparse-mode source register states. Range is 0 to 75000.

Command Default

number : 20000

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **maximum register-states** command is used to set an upper limit for PIM register states. When the limit is reached, PIM discontinues route creation from PIM register messages.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the upper limit for PIM register states to 10000:

```
RP/0/# router pim
RP/0/(config-pim-default-ipv4)# maximum register-states 10000
```

Related Commands

Command	Description
show pim summary, on page 180	Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.

maximum route-interfaces

To configure the maximum number of route interface states that is allowed by Protocol Independent Multicast (PIM), use the **maximum route-interfaces** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

maximum route-interfaces *number*
no maximum route-interfaces

Syntax Description

number	Maximum number of PIM route interface states. Range is 1 to 600000.

Command Default

number : 30000

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **maximum route-interfaces** command is used to set an upper limit for route interface states. When the limit is reached, PIM discontinues route interface creation for its topology table.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the upper limit for PIM route interface states to 200000:

```
RP/0/# router pim
RP/0/(config-pim-default-ipv4)# maximum route-interfaces 200000
```

Related Commands

Command	Description
show pim summary, on page 180	Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.

maximum routes

To configure the maximum number of routes that is allowed by Protocol Independent Multicast (PIM), use the **maximum routes** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

maximum routes *number*
no maximum routes

Syntax Description

number	Maximum number of PIM routes. Range is 1 to 200000.

Command Default

number : 100000

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **maximum routes** command is used to set an upper limit for PIM routes. When the limit is reached, PIM discontinues route creation for its topology table.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the upper limit for PIM routes to 200000:

```
RP/0/# router pim
RP/0/(config-pim-default-ipv4)# maximum routes 200000
```

Related Commands

Command	Description
show pim summary, on page 180	Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.

mofrr

To perform a fast convergence (multicast-only fast reroute, or MoFRR) of specified routes or flows when a failure is detected on one of multiple equal-cost paths between the router and the source, use the **mofrr** command under PIM address-family IPv4 configuration submode.

To disable this feature, use the **no** form of this command.

mofrr { **rib** | **protect** } *route-list* **local-fault-only**

Syntax Description

route-list	Specifies the multicast routes (S, G) s to be enabled by MoFRR.
rib	Specifies MoFRR using Routing Information Base (RIB).
protect	Specifies MoFRR using Protection Global Identifier (GID).
local-fault-only	Specifies priority route convergence option in Protection-based MoFRR for local-link failures only.

Command Default

MoFRR is not enabled by default.

If no VRF is specified, the default VRF is operational.

Command Modes

PIM vrf configuration

PIM address-family IPv4 configuration

Command History

Release	Modification
Release 24.2.11	The keyword **protect** was introduced.
Release 7.0.12	This command was introduced.

Usage Guidelines

Configuring the **local-fault-only** option does not optimize the router for remote-fault MoFRR convergences.

Note MoFRR supports all ECMP hashing algorithms except the source-only hash algorithm. The secondary path is chosen by running the same algorithm on the set of paths that does not include the primary path.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure MoFRR using **rib**:

```
Router(config)# router pim
Router(config-pim)# mofrr rib acl-green

Router(config)# router pim
Router(config-pim)# address-family ipv4
Router(config-pim-default-ipv4)# mofrr rib acl-green
```

Examples

The following example shows how to configure MoFRR using **protect**:

```
Router(config)# router pim
Router(config-pim)# mofrr protect acl-green

Router# router pim
Router(config-pim)# address-family ipv4
Router(config-pim-default-ipv4)# mofrr protect acl-green
```

neighbor-check-on-recv enable

To block the receipt of join and prune messages from non-Protocol Independent Multicast (PIM) neighbors, use the **neighbor-check-on-recv enable** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

neighbor-check-on-recv enable
no neighbor-check-on-recv enable

Syntax Description

This command has no keywords or arguments.

Command Default

Join and prune messages that are sent from non-PIM neighbors are received and not rejected.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable PIM neighbor checking on received join and prune messages:

```
RP/0/# router pim
RP/0/(config-pim-default-ipv4)# neighbor-check-on-recv enable
```

Related Commands

Command	Description
neighbor-check-on-send enable , on page 125	Enables Protocol Independent Multicast (PIM) neighbor checking when sending join and prune messages.

neighbor-check-on-send enable

To enable Protocol Independent Multicast (PIM) neighbor checking when sending join and prune messages, use the **neighbor-check-on-send enable** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

neighbor-check-on-send enable
no neighbor-check-on-send enable

Syntax Description

This command has no keywords or arguments.

Command Default

Join and prune messages are sent to non-PIM neighbors.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable PIM neighbor checking when sending join and prune messages:

```
RP/0/# router pim
RP/0/(config-pim-default-ipv4)# neighbor-check-on-send enable
```

Related Commands

Command	Description
neighbor-check-on-recv enable, on page 124	Blocks the receipt of join and prune messages from non-Protocol Independent Multicast (PIM) neighbors.

neighbor-filter

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IP addresses, use the **neighbor-filter** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

neighbor-filter *access-list*
no neighbor-filter

Syntax Description

access-list	Number or name of a standard IP access list that denies PIM packets from a source.

Command Default

PIM neighbor messages are not filtered.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **neighbor-filter** command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in the command are ignored.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure PIM to ignore all hello messages from IP address 10.0.0.1:

```
RP/0/(config-pim-default-ipv4)# neighbor-filter 1
RP/0/(config-pim-default-ipv4)# exit
RP/0/(config)# ipv4 access-list 1
RP/0/(config-ipv4-acl)# deny ipv4 any 10.0.0.1/24
```

nsf lifetime (PIM)

To configure the nonstop forwarding (NSF) timeout value for the Protocol Independent Multicast (PIM) process, use the **nsf lifetime** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

nsf lifetime *seconds*
no nsf lifetime

Syntax Description

seconds	Maximum time for NSF mode in seconds. Range is 10 to 600.

Command Default

seconds : 120

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

While in PIM NSF mode, PIM is recovering multicast routing topology from the network and updating the Multicast Routing Information Base (MRIB). After the PIM NSF timeout value is reached, PIM signals the MRIB and resumes normal operation.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following command shows how to set the PIM NSF timeout value to 30 seconds:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# nsf lifetime 30
```

Related Commands

Command	Description
nsf (multicast)	Turns on NSF capability for the multicast routing system.
show igmp nsf	Displays the state of NSF operation in IGMP.
show mfib nsf	Displays the state of NSF operation for the MFIB line cards.
show mrib nsf	Displays the state of NSF operation in the MRIB.
show pim nsf, on page 166	Displays the state of NSF operation for PIM.

old-register-checksum

To configure a Cisco IOS XR designated router (DRs) in a network where the rendezvous point is running an older version of Cisco IOS software, use the **old-register-checksum** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

old-register-checksum
no old-register-checksum

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Cisco IOS XR software accepts register messages with checksum on the Protocol Independent Multicast (PIM) header and the next 4 bytes only. This differs from the Cisco IOS method that accepts register messages with the entire PIM message for all PIM message types. The **old-register-checksum** command generates and accepts registers compatible with Cisco IOS software. This command is provided entirely for backward compatibility with Cisco IOS implementations.

Note To allow interoperability with Cisco IOS rendezvous points running older software, run this command on all DRs in your network running Cisco IOS XR software. Cisco IOS XR register messages are incompatible with Cisco IOS software.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set a source designated router (DR) to generate a register compatible with an earlier version of Cisco IOS XR PIM rendezvous point:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# old-register-checksum
```

router pim

To enter Protocol Independent Multicast (PIM) configuration mode, use the **router pim** command in global

configuration mode. To return to the default behavior, use the **no** form of this command.

router pim [**address family** {**ipv4** | **ipv6**}]
no router pim [**address family** {**ipv4** | **ipv6**}]

Syntax Description

address-family	(Optional) Specifies which address prefixes to use.
ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.

Command Default

The default is IPv4 address prefixes.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

From PIM configuration mode, you can configure the address of a rendezvous point (RP) for a particular group, configure the nonstop forwarding (NSF) timeout value for the PIM process, and so on.

Task ID

Task ID	Operations
multicast	read, write

Examples

This example shows how to enter PIM configuration mode for IPv4 address prefixes:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)#
```

This example shows how to enter PIM configuration mode for IPv4 address prefixes and specify the **address-family ipv6** keywords:

```
RP/0/(config)# router pim address-family ipv4
RP/0/(config-pim-default-ipv4)#

RP/0/(config)#
RP/0/(config-pim-default-ipv6)#
```

rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group, use the **rp-address** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

rp-address *ip-address* [*group-access-list*] [**override**] [**bidir**]
no rp-address *ip-address* [*group-access-list*] [**override**] [**bidir**]

Syntax Description

ip-address	IP address of a router to be a PIM rendezvous point. This address is a unicast IP address in four-part dotted-decimal notation.
group-access-list	(Optional) Name of an access list that defines for which multicast groups the rendezvous point should be used. This list is a standard IP access list.
override	(Optional) Indicates that if there is a conflict, the rendezvous point configured with this command prevails over the rendezvous point learned through the auto rendezvous point (Auto-RP) or BSR mechanism.
bidir	(Optional) Configures a bidirectional (bidir) rendezvous point.

Command Default

No PIM rendezvous points are preconfigured.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) require the knowledge of the well-known PIM rendezvous point address. The address is learned through Auto-RP, BSR, or is statically configured using this command.

If the optional *group-access-list-number* argument is not specified, the rendezvous point for the group is applied to the entire IP multicast group range (224.0.0.0/4).

You can configure a single rendezvous point to serve more than one group. The group range specified in the access list determines the PIM rendezvous point group mapping. If no access list is specified, the rendezvous point default maps to 224/4.

If the rendezvous point for a group is learned through a dynamic mechanism, such as Auto-RP, this command might not be required. If there is a conflict between the rendezvous point configured with this command and one learned by Auto-RP, the Auto-RP information is used unless the **override** keyword is specified.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the PIM rendezvous point address to 10.0.0.1 for all multicast groups:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# rp-address 10.0.0.1
```

The following example shows how to set the PIM rendezvous point address to 172.16.6.21 for groups 225.2.2.0 - 225.2.2.255:

```
RP/0/(config)# ipv4 access-list 1
RP/0/(config-ipv4-acl)# permit ipv4 any 225.2.2.0 0.0.0.255
RP/0/(config-ipv4-acl)# exit
RP/0/(config)# router pim
RP/0/(config-pim-ipv4)# rp-address 172.16.6.21
RP/0/(config-pim-ipv4)#
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# rp-address 172.16.6.21
```

Related Commands

Command	Description
ipv4 access-list	Defines a standard IP access list. For more information, see

rpf topology route-policy

To assign a route policy in PIM to select a reverse-path forwarding (RPF) topology, use the **rpf topology route-policy** command in PIM command mode. To disable this configuration, use the **no** form of this command.

rpf topology route-policy *policy-name*
no rpf topology route-policy *policy-name*

Syntax Description

policy-name	(Required) Name of the specific route policy that you want PIM to associate with a reverse-path forwarding topology.

Command Default

No default behavior or values

Command Modes

PIM configuration

PIM address-family configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

For information about routing policy commands and how to create a routing policy, see and .

To assign a route policy using an IPv6 address family prefix, you must enter the command as shown in the Examples section.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following examples show how to associate a specific routing policy in PIM with a RPF topology table for IPv4 address family prefixes:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# rpf topology route-policy mypolicy
RP/0/(config)# router pim address-family ipv6
RP/0/(config-pim-default-ipv6)# rpf topology route-policy mypolicy
```

rpf-redirect

To assign a rpf-redirect route policy in PIM, use the **rpf-redirect route-policy** command in PIM command mode. To disable this configuration, use the **no** form of this command.

rpf-redirect route-policy *policy-name*
no rpf-redirect route-policy *policy-name*

Syntax Description

policy-name	(Required) Name of the specific route policy that you want PIM to associate with a reverse-path forwarding topology.

Command Default

No default behavior or values

Command Modes

PIM configuration

PIM address-family configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

For information about routing policy commands and how to create a routing policy, see and .

Task ID

Task ID	Operation
Multicast	read, write

Example

The following example shows how to associate a specific rpf-redirect routing policy to an rpf-redirect bundle for IPv4 address family prefixes:

```
RP/0/(config)# router pim
RP/0/(config-pim)#address-family ipv4
RP/0/(config-pim-default-ipv4)# rpf-redirect route-policy <route-policy>
```

rpf-redirect bundle

To assign a rpf-redirect bundle in PIM, use the **rpf-redirect bundle** command in PIM command mode. To disable this configuration, use the **no** form of this command.

rpf-redirect bundle <*bundle name*>**bandwidth** <*number in kbps*>**threshold** <*number in kbps*>
no rpf-redirect bundle <*bundle name*>**bandwidth** <*number in kbps*>**threshold** <*number in kbps*>

Syntax Description

bundle name	(Required) Name of the specific bundle route policy that you want PIM to associate with a reverse-path forwarding topology.
number in kbps (bandwidth)	(Required) The value of the bandwidth in kbps.
number in kbps (threshold)	(Required) The threshold value of the bandwidth set in kbps.

Command Default

No default behavior or values

Command Modes

PIM configuration

PIM address-family configuration

Interface mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

For information about routing policy commands and how to create a routing policy, see and .

Task ID

Task ID	Operation
Multicast	read, write

Example

The following examples show how to associate a specific routing policy bundle in PIM with a RPF redirect for IPv4 address family prefixes:

The following command adds the **GigBitEthernet0/0/4/7** interface to the PIM bundle **WEST** and allows maximum of **6000 kbps** to be used by multicast, and initiates a syslog, an alarm message when the usage reaches the threshold **5000 kbps**.

```
RP/0/(config)# router pim
RP/0/(config-pim)#address-family ipv4
RP/0/(config-pim-default-ipv4)# hello-interval 1
RP/0/(config-pim-default-ipv4)# join-prune-interval 15
RP/0/(config-pim-default-ipv4)# rpf-redirect route-policy directv
```

```
RP/0/(config-pim-default-ipv4)# nsf lifetime 60
RP/0/(config-pim-default-ipv4)# interface GigabitEthernet0/0/4/7
RP/0/(config-pim-ipv4-if)# enable
RP/0/(config-pim-ipv4-if)# rpf-redirect bundle WEST bandwidth 6000 threshold 5000
```

rp-static-deny

To configure the deny range of the static Protocol Independent Multicast (PIM) rendezvous point (RP), use the **rp-static-deny** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

rp-static-deny *access-list*
no rp-static-deny

Syntax Description

access-list	Name of an access list. This list is a standard IP access list.

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the PIM RP deny range:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# rp-static-deny listA
```

Related Commands

Command	Description
ipv4 access-list	Defines a standard IP access list.

rpf-vector

To enable Reverse Path Forwarding (RPF) vector signaling for Protocol Independent Multicast (PIM), use the **rpf-vector** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

rpf-vector
no rpf-vector

Syntax Description

This command has no keywords or arguments.

Command Default

By default, RPF vector signaling is disabled.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

RPF vector is a PIM proxy that lets core routers without RPF information forward join and prune messages for external sources (for example, a Multiprotocol Label Switching [MPLS]-based BGP-free core, where the MPLS core router is without external routes learned from Border Gateway Protocol [BGP]).

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable RPF vector:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# rpf-vector
```

rpf-vector use-standard-encoding

To enable Reverse Path Forwarding (RPF) vector signaling for Protocol Independent Multicast (PIM) that is RFC compliant, use the **rpf-vector use-standard-encoding** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

rpf-vector use-standard-encoding [**allow-ebgp** | **disable-ibgp**]

Syntax Description

allow-ebgp	(Optional) Allows RPF vector to originate over an eBGP session.
disable-ibgp	(Optional) Disable RPF vector to originate over an iBGP session.

Command Default

By default, RPF vector signaling is disabled.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

RPF vector is a PIM proxy that lets core routers without RPF information forward join and prune messages for external sources (for example, a MPLS-based BGP-free core, where the MPLS core router is without external routes learned from BGP).

The RPF vector feature is RFC compliant. The new IETF standard encodes PIM messages using PIM Hello option 26.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable RPF vector:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# rpf-vector use-standard-encoding
```

show auto-rp candidate-rp

To display the group ranges that this router represents (advertises) as a candidate rendezvous point (RP), use the **show auto-rp candidate-rp** command in EXEC mode

.

show auto-rp [**ipv4**] **candidate-rp**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show auto-rp candidate-rp** command displays all the candidate rendezvous points configured on this router.

Information that is displayed is the time-to-live (TTL) value; the interval from which the rendezvous point announcements were sent; and the mode, such as Protocol Independent Multicast (PIM) sparse mode (SM), to which the rendezvous point belongs.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show auto-rp candidate-rp** command:

```
RP/0/# show auto-rp candidate-rp

Group Range    Mode   Candidate RP   ttl  interval
224.0.0.0/4     SM       10.0.0.6     30      30
```

This table describes the significant fields shown in the display.

Table 16: show auto-rp candidate-rp Field Descriptions

Field	Description
Group Range	Multicast group address and prefix for which this router is advertised as a rendezvous point.
Mode	PIM protocol mode for which this router is advertised as a rendezvous point , either PIM-SM or bidirectional PIM (bidir).
Candidate RP	Address of the interface serving as a rendezvous point for the range.

Field	Description
ttl	TTL scope value (in router hops) for Auto-RP candidate announcement messages sent out from this candidate rendezvous point interface.
interval	Time between candidate rendezvous point announcement messages for this candidate rendezvous point interface.

show pim global summary

To display configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts for all VRFs, use the **show pim global summary** command in .

show pim global summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show pim global summary**command to display global limits that are shared by all VRFs.

Task ID

Task ID	Operation
multicast	read

Examples

The following is sample output from the **show pim global summary** command that shows PIM routes, with the maximum number of routes allowed being 100000:

```
RP/0/# show pim global summary

PIM Global Summary

PIM State Counters
                          Current        Maximum        Warning-threshold
Routes                    8              100000         100000
Topology Interface States 8              300000         300000
SM Registers              0              20000          20000
AutoRP Group Ranges       0              500            450
BSR Group Ranges          0              500            450
BSR C-RP caches           0              100            0
```

This table describes the significant fields shown in the display.

Table 17: show pim global summary Field Descriptions

Field	Description
Routes	Current number of routes (in the PIM topology table) and the maximum allowed before the creation of new routes is prohibited to avoid out-of-resource (OOR) conditions.
Topology Interface States	Current total number of interfaces (in the PIM topology table) present in all route entries and the maximum allowed before the creation of new routes is prohibited to avoid OOR conditions.

Field	Description
SM Registers	Current number of sparse mode route entries from which PIM register messages are received and the maximum allowed before the creation of new register states is prohibited to avoid OOR conditions.
AutoRP Group Ranges	Current number of sparse mode group range-to-rendezvous point mappings learned through the auto-rendezvous point (Auto-RP) mechanism and the maximum allowed before the creation of new group ranges is prohibited to avoid OOR conditions.
Warning-threshold	Maximum number of multicast routes that can be configured per router.
BSR Group Ranges	The number of BSR groups and the maximum set range.
BSR C-RP caches	The number of candidate-RP caches in BSR and the maximum set range.

show pim nsr

To display the nonstop routing (NSR) information for Protocol Independent Multicast (PIM), use the **show pim nsr** command in EXEC mode.

show pim [**ipv4**| **ipv6**] **nsr**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim nsr** command displays the current multicast NSR state for PIM. For multicast NSR, the state may be Ready or Not activated for non-stop routing. The latter state indicates that recovery is in progress due to a failure in the Multicast Routing Information Base (MRIB) or PIM. The total NSR timeout and time remaining are displayed until NSR expiration.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim nsr** command:

```
RP/0/# show pim nsr

PIM NSR Data:
State            : Ready
RMF Timer        : N [-]
RMF Notif done   : Y
Last RMF rdy     : 4w0d [1]
Last RMF not rdy : Never [0]
Last conn up     : Never [0]
Last conn down   : Never [0]
```

This table describes the significant fields shown in the display.

Table 18: show pim nsr Field Descriptions

Field	Description
State	Multicast Non-Stop Routing State: Ready or Not Ready

Field	Description
RMF Timer	Whether RMF timer is running or not, indicates either Yes or No
RMF Notify done	RMF notification received: Yes or No
Last RMF ready	The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF ready notification was received. Yes, No, or Never respectively.
Last RMF not ready	The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF not ready notification was issued.
Last connection up	The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF not ready notification was received.
Last connection down	Whether the Last connection down notification is issued: Yes, No, or Never. The number in the brackets indicate the number of times the RMF not ready notification was received.

Related Commands

Command	Description
show msdp nsr	Displays the state of NSR operation for MSDP.
show mrib nsr	Displays the state of NSR operation in MRIB.
show igmp nsr	Displays the state of NSR operation for IGMP.

show pim rpf-redirect

To display the maximum bandwidth, the bandwidth used by traffic flowing through the local box, and the bandwidth used by other routers sharing the PIM bundle member interfaces of all members of bundles known to the system, use **show pim rpf-redirect** command in EXEC mode.

show pim *ipv4* **rpf-redirect**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read

Example

The following sample output from the **show pim rpf-redirect** command displays statistics about the PIM bundles:

```
RP/0/#show pim rpf-redirect

Mon Aug 11 16:50:35.811 IST

PIM RPF-Redirect bundle database

 Member   Available/Allocated Available/Allocated   Local  / Network   Total
              Bandwidth      Threshold Bandwidth      Bandwidth     Bandwidth
                (Kbps)               (Kbps)            (Kbps)         (Kbps)


Bundle: east

Gi0/0/0/0    100000/100000        80000/80000             0/0         0
```

where, Available/Allocated Bandwidth (kbps) is the total multicast bandwidth (in kbps) available/allocated for multicast transmission; Available/Threshold Bandwidth (kbps) is the multicast bandwidth threshold beyond which the redirects are enabled, displays the available and the threshold bandwidth (kbps); Local/Network Bandwidth (in kbps) is the difference between the Allocated Bandwidth and Available Bandwidth; and the Total Bandwidth (kbps) is represented by the Local/Network Bandwidth.

show pim rpf-redirect route

To display the content of the snooping database, use **show pim rpf-redirect** command in EXEC mode.

show pim *ipv4* **rpf-redirect route**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read

show pim segment-database

To display information about the segment databases configured for Protocol Independent Multicast (PIM), use the **show pim segment-database** command in EXEC mode.

show pim segment-database

Syntax Description

segment-database	Physical database. **Note** Use the **show pim segment-database** command in EXEC mode to see a list of all databases currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim segment-database** command displays information on all PIM-enabled databases, such as Ingress PE, Upstream Info, Upstream Core Added, Downstream Info, and Downstream Core Added.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim segment-database** command on iABR with MLDP between iPE and iABR, and IR between iABR and eABR.

```
RP/0/#show pim segment-database
Mon Nov  2 17:30:44.728 EST

RD: 4:1, Prefix   : [1][4.4.4.4]/40
    Created          : Nov 25 05:51:07.804 (Up: 01:02:13)
    Leaf Type: I-PMSI, UMH: 4.4.4.4, LSM-ID: 524292 (0x80004)
    Upstream Info: 1 [global-id 2]
    Upstream Core Added, S,I Pmsi Received: [0, 1], S/U Leaf Ad Sent: [1,0]
    Downstream Info: 1 [Tunnel:Type 4 IR ID:0x80004 Label 24012]
    Downstream Core Added, S,I Pmsi Sent/Orig: [0/0, 1]
      Leaf AD List:
        Originating router: 2.2.2.2, Label: 24012
```

In the above sample output, `RD: 4:1, Prefix : [1][4.4.4.4]/40` represents the BGP route advertised by iPE with RD 4:1 and loopback address 4.4.4.4, `Leaf Type: I-PMSI, UMH: 4.4.4.4, LSM-ID: 524292 (0x80004)` represents the LSM-ID of downstream core, `Downstream Info: 1 [Tunnel:Type 4 IR ID:0x80004 Label 24012]` represents the Head local-label of the downstream core, and `Originating router: 2.2.2.2, Label: 24012` represents the Outgoing label for the downstream core.

show pim context

To show the reverse path forwarding (RPF) table information configured for a VRF context, use the **show pim context** command in

EXEC mode

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **context**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following example illustrates output from use of the **show pim context** command:

```
RP/0/# show pim   context

VRF ID: 0x60000000
Table ID: 0xe0000000
Remote Table ID: 0xe0800000
MDT Default Group : 0.0.0.0
MDT handle: 0x0
Context Active, ITAL Active
Routing Enabled
Registered with MRIB
Not owner of MDT Interface
Raw socket req: T, act: T, LPTS filter req: T, act: T
UDP socket req: T, act: T, UDP vbind req: T, act: T
Reg Inj socket req: F, act: F, Reg Inj LPTS filter req: F, act: F
Mhost Default Interface : Null (publish pending: F)
Remote MDT Default Group : 0.0.0.0
Neighbor-filter: -
```

The following table gives the field descriptions for the **show pim context** command output:

Table 19: show pim context Field Descriptions

Field	Description
VRF ID	VPN routing and forwarding instance identification.
Table ID	Identification of unicast default table as of VRF context activation.
Remote Table ID	Identifies the table ID of the opposite address family. For example, the remote table ID for the VRF context of the
MDT Default Group	Identifies the multicast distribution tree (MDT) group configured as the default for use by the VRF.
MDT handle	Identifies the handle for multicast packets to be passed through the MDT interface.
Context Active	Identifies whether or not the VRF context was activated.
ITAL Active	Identifies whether or not the VRF is registered with ITAL. If it is, this signifies that the VRF is configured globally.
Routing Enabled	Identifies whether or not PIM is enabled in the VRF.
Registered with MRIB	Identifies whether or not the VRF is registered with Multicast Routing Information Base (MRIB).
Not owner of MDT interface	Identifies a process as not being the owner of the MDT interface. The owner is either the PIM or the PIM IPv6 process.
Owner of MDT interface	Identifies the owner of the MDT interface. The owner is either the PIM or the PIM IPv6 process.
Raw socket req:	Raw socket operations requested.
act:	Action: Indicates whether or not the operations were performed.
T; F	True; False
LPTS filter req	Identifies whether or not the VRF was requested to be added to the socket.
UDP socket req	Identifies whether or not a UDP socket was requested.
UDP vbind req	Identifies whether or not the VRF was added to the UDP socket.
Reg Inj socket req	This Boolean indicates whether or not the register inject socket, used for PIM register messages, was requested.
Reg Inj LPTS filter req	Indicates whether or not the VRF was added to the register inject socket.
Mhost Default Interface	Identifies the default interface to be used for multicast host (Mhost).

Field	Description
Remote MDT Default Group	Identifies the MDT transiting this VRF or address family in use by the remote address family.
Neighbor-filter	Name of the neighbor filter used to filter joins or prunes from neighbors. If the there is no neighbor filter, the output reads: "-".

show pim context table

To display a summary list of all tables currently configured for a VRF context, use the **show pim context table** command in

EXEC mode

.

show pim [**vrf vrf-name**] [**ipv4**] **context table**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following example illustrates the output for PIM table contexts for a VRF default after using the **show pim context table** command:

RP/0/ RSP0 /CPU0:router# **show pim ipv4 context table**

```
PIM Table contexts for VRF default

Table                               TableID       Status
IPv4-Unicast-default                0xe0000000    Active
IPv4-Multicast-default              0xe0100000    Active
IPv4-Multicast-t201                 0xe010000b    Active
IPv4-Multicast-t202                 0xe010000c    Active
IPv4-Multicast-t203                 0xe010000d    Active
IPv4-Multicast-t204                 0xe010000e    Active
IPv4-Multicast-t205                 0xe010000f    Active
IPv4-Multicast-t206                 0xe0100010    Active
IPv4-Multicast-t207                 0xe0100011    Active
IPv4-Multicast-t208                 0x00000000    Inactive
IPv4-Multicast-t209                 0x00000000    Inactive
IPv4-Multicast-t210                 0x00000000    Inactive
```

Table 20: show pim ipv4 context table Field Descriptions

Field	Description
Table	Context table name.
Table ID	RSI table ID for the table.
Status	Identifies whether or not the context table is active or inactive. The table displays “Active” if it was globally configured under a given VRF, and if RSI considers it to be active. The table displays “Inactive” if the opposite is true.

show pim group-map

To display group-to-PIM mode mapping, use the **show pim group-map** command in

EXEC

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **group-map** [*ip-address-name*] [**info-source**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ip-address-name	(Optional) IP address name as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4** host in the format *A.B.C.D.*
info-source	(Optional) Displays the group range information source.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim group-map** command displays all group protocol address mappings for the rendezvous point. Mappings are learned from different clients or through the auto rendezvous point (Auto-RP) mechanism.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim group-map** command:

```
RP/0/# show pim group-map

IP PIM Group Mapping Table
(* indicates group mappings being used)
(+ indicates BSR group mappings active in MRIB)

Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    perm   1      0.0.0.0
224.0.1.40/32*      DM    perm   1      0.0.0.0
224.0.0.0/24*       NO    perm   0      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    autorp 1      10.10.2.2       RPF: POS01/0/3,10.10.3.2
224.0.0.0/4         SM    static        0 0.0.0.0       RPF: Null,0.0.0.0
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the Protocol Independent Multicast (PIM) Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

Line 5 shows that all the remaining groups are in sparse mode mapped to rendezvous point 10.10.3.2.

This table describes the significant fields shown in the display.

Table 21: show pim group-map Field Descriptions

Field	Description
Group Range	Multicast group range that is mapped.
Proto	Multicast forwarding mode.
Client	States how the client was learned.
Groups	Number of groups from the PIM topology table.
RP address	Rendezvous point address.
Info	RPF interface used and the PIM-SM Reverse Path Forwarding (RPF) information toward the rendezvous point.

Related Commands

Command	Description
domain ipv4 host	Defines a static hostname-to-address mapping in the host cache using IPv4. For more information, see
rp-address, on page 130	Configures the address of a PIM rendezvous point for a particular group.
show pim range-list, on page 168	Displays the range-list information for PIM.

show pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show pim interface** command in

EXEC

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **interface** [*type interface-path-id* | **state-on** | **state-off**] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
state-on	(Optional) Displays only interfaces from which PIM is enabled and active.
state-off	(Optional) Displays only interfaces from which PIM is disabled or inactive.
detail	(Optional) Displays detailed address information.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim interface** command displays neighboring information on all PIM-enabled interfaces, such as designated router (DR) priority and DR election winner.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim interface** command:

```
RP/0/# show pim interface

Address                         Interface              PIM  Nbr   Hello  DR    DR
                                                           Count Intvl  Prior
172.29.52.127                   MgmtEth0/0/CPU0/0      off  0     30     1     not elected
10.6.6.6                        Loopback0              off  0     30     1     not elected
0.0.0.0                         Loopback60             off  0     30     1     not elected
0.0.0.0                         Loopback61             off  0     30     1     not elected
10.46.4.6                       ATM0/2/0/0.1           off  0     30     1     not elected
10.46.5.6                       ATM0/2/0/0.2           off  0     30     1     not elected
10.46.6.6                       ATM0/2/0/0.3           off  0     30     1     not elected
10.46.7.6                       ATM0/2/0/0.4           off  0     30     1     not elected
10.46.8.6                       ATM0/2/0/3.1           off  0     30     1     not elected
10.46.9.6                       ATM0/2/0/3.2           off  0     30     1     not elected
10.56.16.6                      Serial0/3/2/1          off  0     30     1     not elected
10.56.4.2                       Serial0/3/0/0/0:0      off  0     30     1     not elected
10.56.4.6                       Serial0/3/0/0/1:0      off  0     30     1     not elected
10.56.4.10                      Serial0/3/0/0/2:0      off  0     30     1     not elected
10.56.4.14                      Serial0/3/0/0/2:1      off  0     30     1     not elected
10.56.4.18                      Serial0/3/0/0/3:0      off  0     30     1     not elected
10.56.4.22                      Serial0/3/0/0/3:1      off  0     30     1     not elected
10.56.4.26                      Serial0/3/0/0/3:2      off  0     30     1     not elected
10.56.4.30                      Serial0/3/0/0/3:3      off  0     30     1     not elected
10.56.8.2                       Serial0/3/0/1/0:0      off  0     30     1     not elected
10.56.12.6                      Serial0/3/2/0.1        off  0     30     1     not elected
10.56.13.6                      Serial0/3/2/0.2        off  0     30     1     not elected
10.56.14.6                      Serial0/3/2/0.3        off  0     30     1     not elected
10.56.15.6                      Serial0/3/2/0.4        off  0     30     1     not elected
10.67.4.6                       POS0/4/1/0             off  0     30     1     not elected
10.67.8.6                       POS0/4/1/1             off  0     30     1     not elected
```

This table describes the significant fields shown in the display.

Table 22: show pim interface Field Descriptions

Field	Description
Address	IP address of the interface.
Interface	Interface type and number that is configured to run PIM.
PIM	PIM is turned off or turned on this interface.
Nbr Count	Number of PIM neighbors in the neighbor table for the interface.
Hello Intvl	Frequency, in seconds, of PIM hello messages, as set by the **ip pim hello-interval** command in interface configuration mode.
DR Priority	Designated router priority is advertised by the neighbor in its hello messages.

Field	Description
DR	IP address of the DR on the LAN. Note that serial lines do not have DRs, so the IP address is shown as 0.0.0.0. If the interface on this router is the DR, “this system” is indicated; otherwise, the IP address of the external neighbor is given.

Related Commands

Command	Description
show pim neighbor, on page 163	Displays the Protocol Independent Multicast (PIM) neighbors discovered by means of PIM hello messages.

show pim join-prune statistic

To display Protocol Independent Multicast (PIM) join and prune aggregation statistics, use the **show pim join-prune statistics** command in EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **join-prune statistic** [*type interface-path-id*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

IP addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim join-prune statistics** command displays the average PIM join and prune groups for the most recent packets (in increments of 1000/10000/50000) that either were sent out or received from each PIM interface. If fewer than 1000/10000/50000 join and prune group messages are received since PIM was started or the statistics were cleared, the join-prune aggregation shown in the command display is zero (0).

Because each PIM join and prune packet can contain multiple groups, this command can provide a snapshot view of the average pace based on the number of join and prune packets, and on the consideration of the aggregation factor of each join and prune packet.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim join-prune statistics** command with all router interfaces specified:

```
RP/0/# show pim join-prune statistics
```

```
PIM Average Join/Prune Aggregation for last (100/1K/10K) packets
Interface      MTU    Transmitted    Received

Loopback0      1514   0 / 0 / 0      0 / 0 / 0
Encapstunnel0  0      0 / 0 / 0      0 / 0 / 0
Decapstunnel0  0      0 / 0 / 0      0 / 0 / 0
Loopback1      1514   0 / 0 / 0      0 / 0 / 0
POS0/3/0/0     4470   0 / 0 / 0      0 / 0 / 0
POS0/3/0/3     4470   0 / 0 / 0      0 / 0 / 0
```

This table describes the significant fields shown in the display.

Table 23: show pim join-prune statistics Field Descriptions

Field	Description
Interface	Interface from which statistics were collected.
MTU	Maximum transmission unit (MTU) in bytes for the interface.
Transmitted	Number of join and prune states aggregated into transmitted messages in the last 1000/10000/50000 transmitted join and prune messages.
Received	Number of join and prune states aggregated into received messages in the last 1000/10000/50000 received join and prune messages.

show pim mstatic

To display multicast static routing information, use the **show pim mstatic** command in

EXEC

mode.

show pim [**ipv4**] **mstatic** [**ipv4**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim mstatic** command is used to view all the multicast static routes. Multicast static routes are defined by the **static-rpf** command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim mstatic** command that shows how to reach IP address 10.0.0.1:

```
RP/0/# show pim mstatic

IP Multicast Static Routes Information
* 10.0.0.1/32 via pos0/1/0/1 with nexthop 172.16.0.1 and distance 0
```

This table describes the significant fields shown in the display.

Table 24: show pim mstatic Field Descriptions

Field	Description
10.0.0.1	Destination IP address.
pos0/1/0/1	Interface that is entered to reach destination IP address 10.0.0.1
172.16.0.1	Next-hop IP address to enter to reach destination address 10.0.0.1.
0	Distance of this mstatic route.

Related Commands

Command	Description
static-rpf	Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.

show pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by means of PIM hello messages, use the **show pim neighbor** command in

EXEC

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **neighbor** [*type interface-path-id*] [**count** | **detail**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
count	(Optional) Number of neighbors present on the specified interface, or on all interfaces if one is not specified. The interface on this router counts as one neighbor in the total count.
detail	(Optional) Displays detailed information.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim neighbor** command:

```
RP/0/# show pim neighbor

Neighbor Address  Interface              Uptime    Expires DR pri Bidir

172.17.1.2*       Loopback1              03:41:22  00:01:43 1 (DR) B
172.17.2.2*       Loopback2              03:41:20  00:01:31 1 (DR) B
172.17.3.2*       Loopback3              03:41:18  00:01:28 1 (DR) B
10.10.1.1         POS0/2/0/0             03:40:36  00:01:41 1      B
10.10.1.2*        POS0/2/0/0             03:41:28  00:01:32 1 (DR) B
10.10.2.2*        POS0/2/0/2             03:41:26  00:01:36 1      B
10.10.2.3         POS0/2/0/2             03:41:25  00:01:29 1 (DR) B
PIM neighbors in VRF default

Neighbor Address             Interface              Uptime    Expires  DR pri
Flags

10.6.6.6*                    Loopback0              4w1d      00:01:24 1 (DR) B
10.16.8.1                    GigabitEthernet0/4/0/2 3w2d      00:01:24 1      B
10.16.8.6*                   GigabitEthernet0/4/0/2 3w2d      00:01:28 1 (DR) B
192.168.66.6*                GigabitEthernet0/4/0/0.7 4w1d      00:01:28 1 (DR)
B P
192.168.67.6*                GigabitEthernet0/4/0/0.8 4w1d      00:01:40 1 (DR)
B P
192.168.68.6*                GigabitEthernet0/4/0/0.9 4w1d      00:01:24 1 (DR)
B P

PIM neighbors in VRF default

Neighbor Address  Interface                Uptime    Expires       DR     pri Flags

28.28.9.2*        GigabitEthernet0/2/0/9   00:39:34  00:01:40 1   (DR)     B  A
10.1.1.1          GigabitEthernet0/2/0/19  00:49:30  00:01:42 1            B  A
10.1.1.2*         GigabitEthernet0/2/0/19  00:50:01  00:01:41 1   (DR)     B  A
2.2.2.2*          Loopback0                00:50:01  00:01:42 1   (DR)     B  A
```

The following is sample output from the **show pim neighbor** command with the **count** option:

```
RP/0/# show pim neighbor count

Interface   Nbr count
POS0/3/0/0     1
Loopback1      1
Total Nbrs     2
```

This table describes the significant fields shown in the display.

Table 25: show pim neighbor Field Descriptions

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	Time the entry has been in the PIM neighbor table.
Expires	Time until the entry is removed from the IP multicast routing table.

Field	Description
DR pri	DR priority sent by the neighbor in its hello messages. If this neighbor is elected as the DR on the interface, it is annotated with "(DR)" in the command display.
Nbr count	Number of PIM neighbors in the neighbor table for all interfaces on this router.

Related Commands

Command	Description
show pim interface, on page 156	Displays information about interfaces configured for Protocol Independent Multicast (PIM).

show pim nsf

To display the state of nonstop forwarding (NSF) operation for Protocol Independent Multicast (PIM), use the **show pim nsf** command in

EXEC
mode

.

show pim [**ipv4**] **nsf**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim nsf** command displays the current multicast NSF state for PIM. For multicast NSF, the state may be normal or activated for nonstop forwarding. The latter state indicates that recovery is in progress due to a failure in the Multicast Routing Information Base (MRIB) or PIM. The total NSF timeout and time remaining are displayed until NSF expiration.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim nsf** command:

```
RP/0/# show pim nsf

IP PIM Non-Stop Forwarding Status:
Multicast routing state: Non-Stop Forwarding Activated
NSF Lifetime: 00:02:00
NSF Time Remaining: 00:01:56
```

This table describes the significant fields shown in the display.

Table 26: show pim nsf Field Descriptions

Field	Description
Multicast routing state	PIM state is in NSF recovery mode (Normal or Non-Stop Forwarding Activated).
NSF Lifetime	Total NSF lifetime (seconds, hours, and minutes) configured for PIM.

Field	Description
NSF Time Remaining	Time remaining in NSF recovery for PIM if NSF recovery is activated.

show pim range-list

To display range-list information for Protocol Independent Multicast (PIM), use the **show pim range-list** command in

EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**] **range-list** [**config**] [*ip-address-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
config	(Optional) Displays PIM command-line interface (CLI) range list information.
ip-address-name	(Optional) IP address of the rendezvous point.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim range-list** command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable. The **config** keyword means that the particular range is statically configured.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim range-list** command:

```
RP/0/# show pim range-list


config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

This table describes the significant fields shown in the display.

Table 27: show pim range-list Field Descriptions

Field	Description
config	Group range was learned by means of configuration.
SSM	PIM mode is operating in Source Specific Multicast (SSM) mode. Other modes are Sparse-Mode (SM) and bidirectional (BD) mode.
Exp: never	Expiration time for the range is “never”.
Src: 0.0.0.0	Advertising source of the range.
230.0.0.0/8	Group range: address and prefix.
Up: 03:47:09	Total time that the range has existed in the PIM group range table. In other words, the uptime in hours, minutes, and seconds.

Related Commands

Command	Description
show pim group-map, on page 154	Displays group-to-PIM mode mapping.

show pim rpf

To display information about reverse-path forwarding (RPF) in one or more routing tables within Protocol Independent Multicast (PIM), use the **show pim rpf** command in

EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**] {**multicast** | **safi-all** | **unicast**} [**topology** {*tablename* | **all**}] **rpf** [*ip-address* / *name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
multicast	(Optional) Specifies a multicast secondary address family (SAFI).
safi-all	(Optional) Specifies a secondary address family (SAFI) wildcard.
unicast	(Optional) Specifies a unicast secondary address family (SAFI).
topology	(Optional) Specifies the display of multitopology routing table information.
table-name	Name of the specific multitopology table to show.
all	Specifies that detailed information be displayed for all multitopology routing tables in PIM.
ip-address/name	(Optional) IP address or name, or both, for the default or selected route policy with the domain IPv4 host in the format *A.B.C.D.* **Note** The *ip-address* argument can also be a Protocol Independent Multicast (PIM) rendezvous point (RP) address.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following example shows output from the **show pim rpf** command:

```
RP/0/# show pim rpf

Table: IPv4-Unicast-default
* 61.61.1.10/32 [90/181760]
    via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
    via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
    via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
* 61.61.1.91/32 [90/181760]
    via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
    via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
    via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
* 61.61.1.92/32 [90/181760]
    via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
    via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
    via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
* 61.61.1.93/32 [90/181760]
    via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
    via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
    via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
```

show pim rpf hash

To display information for Routing Information Base (RIB) lookups used to predict RPF next-hop paths for routing tables in Protocol Independent Multicast (PIM), use the **show pim rpf hash** command in

EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**] [**multicast** | **safi-all** | **unicast**] [**topology** {*table-name* | **all**}] **rpf hash** *root / group ip-address / name* [**hash-mask-length** *bit-length* | **mofrr**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
multicast	(Optional) Specifies a multicast secondary address family (SAFI).
safi-all	(Optional) Specifies a secondary address family (SAFI) wildcard.
unicast	(Optional) Specifies a unicast secondary address family (SAFI).
topology	(Optional) Specifies the display of multitopology routing table information.
table-name	Name of the specific multitopology table to show.
all	Specifies that detailed information be displayed for all multitopology routing tables in PIM.
root/group ip-address / *group-name*	Root or group address, or both, for the default or selected route policy. IP address is as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4** host in the format *A.B.C.D.*
hash-mask-length *bit-length*	(Optional) Specifies the bootstrap router (BSR) hash mask length to be applied to the next-hop hashing. Default is the BSR hash mask length known for the matching group range (or host mask length if BSR is not configured for the range). The range in bit length is 0 to 32.
mofrr	(Optional) Specifies MOFRR hashing.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim rpf hash** command lets you predict the way routes balance across Equal-Cost Multipath (ECMP) next hops. It does not require that route to exist in the Multicast Routing Information Base (MRIB) at the time.

When using the *ip-address* argument for a (*,G) route, use the rendezvous point address and omit the *group-address* argument. For (S,G) routes, use the *ip-address* and the *group-address* arguments.

Task ID

Task ID	Operations
multicast	read

Examples

When you use the **show pim rpf hash** command, Cisco IOS XR software displays statistics regarding route policy invocations in topology tables:

```
RP/0/# show pim rpf hash 10.0.0.1 239.0.0.1

Multipath RPF selection is enabled.

RPF next-hop neighbor selection result: POS0/2/0/0,10.1.0.1
```

The following example shows the results from use of the **mofrr** keyword:

```
RP/0/# show pim rpf hash 11.11.0.4 226.1.1.2 mofrr

Table: IPv4-Unicast-default
Multipath RPF selection is enabled.
RPF next-hop neighbor selection result:
GigabitEthernet0/4/0/4,55.55.55.101
Secondary RPF next-hop neighbor selection result:
GigabitEthernet0/4/0/4,55.55.55.101
```

Related Commands

Command	Description
show pim rpf, on page 170	Displays information about reverse-path forwarding (RPF) in one or more routing tables within Protocol Independent Multicast (PIM).

show pim rpf route-policy statistics

To display statistics for reverse-path forwarding (RPF) route policy invocations in Protocol Independent Multicast (PIM) routing tables, use the **show pim rpf route-policy statistics** command in

EXEC mode

.

show pim [**vrf vrf-name**] [**ipv4**] **rpf route-policy statistics**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following sample output from the **show pim rpf route-policy statistics** command displays statistics about route policy invocations in topology tables:

```
RP/0/# show pim mt4-p201 rpf route-policy statistics

RPF route-policy statistics for VRF default:
    Route-policy name: mt4-p201
    Number of lookup requests 25
    Pass 25, Drop 0
    Default RPF Table selection 5, Specific RPF Table selection 20
```

This table describes the significant fields shown in the display.

Table 28: show pim rpf route-policy statistics Field Description

Field	Description
Route-policy name	Name of a specific route policy.
Number of lookup requests	Number of times the route policy was run to determine the RPF table.

Field	Description
Pass	Number of (S,G) entries that were passed by the route policy.
Drop	Number of (S,G) entries that were dropped by the route policy.
Default RPF Table selection/Specific RPF Table selection	When an (S,G) entry is accepted by the route policy, it can either select the default RPF table (can be either the unicast default or multicast default table) or any specific named or default RPF table. The last line of output indicates the number of entries that fall into these two categories.

show pim rpf route-policy test

To test the outcome of a route-policy with reverse-path forwarding (RPF), use the **show pim rpf route-policy test** command in EXEC mode.

show pim [*vrf* **vrf-name**] [**ipv4**] **rpf route-policy test** *src-ip-address / grp-address*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
src-ip-address/ grp-address	Source or group address, or both, for the default or selected route policy, as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D.*

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following sample output from the **show pim rpf route-policy test** command displays the RPF table selected by the route policy for a given source and/or group address:

```
RP/0/# show pim ipv4 rpf route-policy test 10.11.11.11 225.2.0.1


RPF route-policy test for VRF default:
    Route-policy name: mt4-p2
    Source 10.11.11.11, Group 225.2.0.1
    Result: Pass
    Default RPF Table selected
    RPF Table: IPv4-Unicast-default  (Created, Active)
```

This table describes the significant fields shown in the display.

Table 29: show pim rpf route-policy test Field Descriptions

Field	Description
Route-policy name	Name of a specific route policy.
Source	Source IP name for the route policy.
Group	Group IP name for the route policy.
Result	Specifies whether the (S,G) entry was accepted by the route policy.
Default RPF Table	Specifies whether the (S,G) entry uses the default or a specific RPF table.
RPF Table	Specifies which RPF table was selected, and whether or not the table was created in PIM and is active.

show pim rpf summary

To display summary information about the interaction of Protocol Independent Multicast (PIM) with the Routing Information Base (RIB), including the convergence state, current default RPF table, and the number of source or rendezvous point registrations created, use the **show pim rpf summary** command in EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**] [**multicast** | **safi-all** | **unicast**] [**topology** {*table-name* | **all**}] **rpf summary**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
multicast	(Optional) Specifies a multicast secondary address family (SAFI).
safi-all	(Optional) Specifies a secondary address family (SAFI) wildcard.
unicast	(Optional) Specifies a unicast secondary address family (SAFI).
topology	(Optional) Specifies the display of multitopology routing table information.
table-name	Name of the specific multitopology table to show.
all	Specifies that detailed information be displayed for all multitopology routing tables in PIM.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following sample output shows RPF information for multiple tables. The first part of the output example describes VRF-level information. The remainder consists of information specific to one or more tables.

Note RPF table indicates the table in which the RPF lookup was performed for this route entry.

```
RP/0/# show pim ipv4 unicast topology all rpf summary


MBGP                Not configured
    OSPF Mcast-intact   Not configured
    ISIS Mcast-intact   Not configured
    ISIS Mcast Topology Not configured

PIM RPFs registered with Unicast RIB table

Default RPF Table: IPv4-Unicast-default
RIB Convergence Timeout Value: 00:30:00
RIB Convergence Time Left:     00:00:00
Multipath RPF Selection is Enabled

Table: IPv4-Multicast-default
    PIM RPF Registrations = 0
    RIB Table converged

Table: IPv4-Multicast-t300
    PIM RPF Registrations = 3
    RIB Table converged

Table: IPv4-Multicast-t310
    PIM RPF Registrations = 5
    RIB Table converged

Table: IPv4-Multicast-t320
    PIM RPF Registrations = 5
    RIB Table converged
```

The first part of the output example describes VRF-level information. The remainder consists of information specific to one or more tables.

The following example shows the sample output for **show pim rpf summary** command:

```
RP/0/# show pim rpf summary


    MBGP                Not configured
    OSPF Mcast-intact   Configured
    ISIS Mcast-intact   Not configured
    ISIS Mcast Topology Not configured
    MoFRR Flow-based    Configured
    MoFRR RIB           Not configured

PIM RPFs registered with Multicast RIB table

Default RPF Table: IPv4-Multicast-default
RIB Convergence Timeout Value: 00:30:00
RIB Convergence Time Left:     00:00:00
Multipath RPF Selection is Disabled

Table: IPv4-Multicast-default
    PIM RPF Registrations = 3
    RIB Table converged
```

show pim summary

To display configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts, use the **show pim summary** command in .

show pim [**vrf** *vrf-name*] [**ipv4**] **summary**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance associated with this count.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show pim summary** command is used to identify configured OOR information for the PIM protocol, such as number of current and maximum routes.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim summary** command that shows PIM routes, with the maximum number of routes allowed being 100000:

```
RP/0/# show pim summary

PPIM Summary for VRF:default

PIM State Counters
                          Current        Maximum        Warning-threshold
Routes                    4              100000         100000
Topology Interface States 4              300000         300000
SM Registers              1              20000          20000
AutoRP Group Ranges       0              500            450
BSR Group Ranges          9              500            450
BSR C-RP caches           9              100            100
```

This table describes the significant fields shown in the display.

Table 30: show pim summary Field Descriptions

Field	Description
Routes	Current number of routes (in the PIM topology table) and the maximum allowed before the creation of new routes is prohibited to avoid out-of-resource (OOR) conditions.
Routes x Interfaces	Current total number of interfaces (in the PIM topology table) present in all route entries and the maximum allowed before the creation of new routes is prohibited to avoid OOR conditions.
SM Registers	Current number of sparse mode route entries from which PIM register messages are received and the maximum allowed before the creation of new register states is prohibited to avoid OOR conditions.
AutoRP Group Ranges	Current number of sparse mode group range-to-rendezvous point mappings learned through the auto-rendezvous point (Auto-RP) mechanism and the maximum allowed before the creation of new group ranges is prohibited to avoid OOR conditions.
Warning-threshold	Maximum number of multicast routes that can be configured per router.
BSR Group Ranges	The number of BSR groups and the set range.
BSR C-RP caches	The number of candidate-RP caches in BSR and the set range.

show pim topology

To display Protocol Independent Multicast (PIM) routing topology table information for a specific group or all groups, use the **show pim topology** command in

EXEC

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **topology** [*src-ip-address*/*grp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
src-ip-address/ grp-address	Source IP address or group IP address, as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the PIM routing topology table to display various entries for a given group, (*, G), (S, G), and

(S, G) RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

When multicast-only fast reroute (MoFRR) feature is enabled, the **show pim topology** command shows the SGs that are configured for MoFRR. For information about the MoFRR primary and secondary paths, see the description of the command show pim topology detail, on page 188.

Note For forwarding information, use the **show mfib route** and **show mrib route** commands.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim topology** command:

```
RP/0/# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
 RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
 RR - Register Received, SR - Sending Registers, E - MSDP External, EX - Extranet
 DCC - Don't Check Connected,
 ME - MDT Encap, MD - MDT Decap,
MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
 II - Internal Interest, ID - Internal Dissinterest,
 LH - Last Hop, AS - Assert, AB - Admin Boundary

(11.0.0.1,239.9.9.9)SPT SM Up: 00:00:13
JP: Join(never) RPF: Loopback1,11.0.0.1* Flags: KAT(00:03:16) RA RR
No interfaces in immediate olist

(*,239.9.9.9) SM Up: 4d14h RP: 11.0.0.1*
JP: Join(never) RPF: Decapstunnel0,11.0.0.1 Flags: LH
POS0/3/0/0 4d14h fwd LI II LH

(*,224.0.1.39) DM Up: 02:10:38 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
  POS0/2/0/0 02:10:38  off LI II LH

(*,224.0.1.40) DM Up: 03:54:23 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
  POS0/2/0/0 03:54:23  off LI II LH
  POS0/2/0/2               03:54:14  off LI
  POS0/4/0/0 03:53:37  off LI

(*,239.100.1.1) BD Up: 03:51:35 RP: 200.6.1.6
JP: Join(00:00:24) RPF: POS0/4/0/0,10.10.4.6 Flags:
  POS0/2/0/0 03:42:05  fwd Join(00:03:18)
  POS0/2/0/2               03:51:35  fwd Join(00:02:54)
(*,235.1.1.1) SM Up: 03:51:39 RP: 200.6.2.6
JP: Join(00:00:50) RPF: POS0/4/0/0,10.10.4.6 Flags:
  POS0/2/0/2               02:36:09  fwd Join(00:03:20)
  POS0/2/0/0 03:42:04  fwd Join(00:03:16)
```

The following example shows output for a MoFRR convergence:

```
RP/0/# show pim topology 239.1.1.1

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    MF – MOFRR Enabled, MFP – Primary MoFRR,
    MFB – Backup MoFRR, MFA – Active MoFRR,

    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected,
    ME - MDT Encap, MD - MDT Decap,
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
```

```
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1)SPT SSM Up: 13:54:06
JP: Join(00:00:41) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
  GigabitEthernet0/5/0/1      13:54:06  fwd LI LH
RP/0/4/CPU0:Sunnyvale#show pim topology 239.1.1.1 detail

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected,
    ME - MDT Encap, MD - MDT Decap,
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1)SPT SSM Up: 13:54:10
JP: Join(00:00:37) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/5/0/3.2,100.100.200.10
  GigabitEthernet0/5/0/1      13:54:10  fwd LI LH
```

The following example shows a sample output for flow-based MoFRR:

```
RP/0/# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources,  RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(*,224.0.1.40) DM Up: 00:31:45 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
  GigabitEthernet0/0/0/8      00:31:45  off LI II LH

(20.20.20.1,225.0.0.1)SPT SM Up: 00:31:39
JP: Join(00:00:09) RPF: GigabitEthernet0/0/0/8,20.20.20.1 MoFRR, Flags:
  GigabitEthernet0/0/0/28     00:31:39  fwd LI LH

(20.20.20.1,225.0.0.2)SPT SM Up: 00:31:39
JP: Join(00:00:09) RPF: GigabitEthernet0/0/0/8,20.20.20.1 MoFRR, Flags:
  GigabitEthernet0/0/0/28     00:31:39  fwd LI LH
```

If the option detail is issued, then the secondary RPF of MoFRR route will be shown in the console.

```
RP/0/# show pim topology detail

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
```

```
    DSS - Don't Signal Sources,  RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(*,224.0.1.40) DM Up: 03:16:10 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
RPF Table: None
  GigabitEthernet0/0/0/8      03:16:10  off LI II LH

(20.20.20.1,225.0.0.1)SPT SM Up: 03:16:04
JP: Join(00:00:45) RPF: GigabitEthernet0/0/0/8,20.20.20.1 MoFRR, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/0/0/18,20.20.20.1
  GigabitEthernet0/0/0/28     03:16:04  fwd LI LH

(20.20.20.1,225.0.0.2)SPT SM Up: 03:16:04
JP: Join(00:00:45) RPF: GigabitEthernet0/0/0/8,20.20.20.1 MoFRR, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/0/0/18,20.20.20.1
  GigabitEthernet0/0/0/28     03:16:04  fwd LI LH
```

This table describes the significant fields shown in the display. It includes fields that do not appear in the example, but that may appear in your output.

Table 31: show pim topology Field Descriptions

Field	Description
(11.0.0.1,239.9.9.9)SPT	Entry state. Source address, group address, and tree flag (shortest path tree or rendezvous point tree) for the route entry. Note that the tree flag may be missing from the entry.
SM	Entry protocol. PIM protocol mode in which the entry operates: sparse mode (SM), source specific multicast (SSM), bidirectional (BD), or dense-mode (DM).
Up: 00:00:13	Entry uptime. Time (in hours, minutes, and seconds) this entry has existed in the topology table.
RP: 11.0.0.1*	Entry information. Additional information about the route entry. If route entry is a sparse mode or bidirectional PIM route, the RP address is given.
JP: Null(never)	Entry join/prune state. Indicates if and when a join or prune message is sent to the RPF neighbor for the route.
MoFRR RIB, Flags:	Indicates whether the (S,G) route is a RIB-based MoFRR route.
MoFRR, Flags:	Indicates whether the (S,G) route is a flow-based MoFRR route. By default, a flow-based MoFRR route will be a RIB-based MoFRR route but not in the reverse way.
RPF Table	IPv4 Unicast default.
RPF Secondary	Secondary path interface

Field	Description
Entry Information Flags	
KAT - Keep Alive Timer	The keepalive timer tracks whether traffic is flowing for the (S, G) route on which it is set. A route does not time out while the KAT is running. The KAT runs for 3.5 minutes, and the route goes into KAT probing mode for as long as 65 seconds. The route is deleted if no traffic is seen during the probing interval, and there is no longer any reason to keep the route—for example, registers and (S, G) joins.
AA - Assume Alive	Flag that indicates that the route was alive, but recent confirmation of traffic flow was not received.
PA - Probe Alive	Flag that indicates that the route is probing the data plane to determine if traffic is still flowing for this route before it is timed out.
RA - Really Alive	Flag that indicates that the source is confirmed to be sending traffic for the route.
LH - Last Hop	Flag that indicates that the entry is the last-hop router for the entry. If (S, G) routes inherit the LH olist from an (*, G) route, the route entry LH flag appears only on the (*, G) route.
IA - Inherit Alive	Flag that indicates a source VPN routing and forwarding (VRF) route with the KAT active.
DSS - Don’t Signal Sources	Flag that may be set on the last-hop (*, G) entries that indicates that new matching sources should not be signaled from the forwarding plane.
DCC - Don’t Check Connected	Flag that is set when the KAT probes, which indicates that the connected check for new sources should be omitted in the forwarding plane.
RR - Register Received	Flag that indicates that the RP has received and answered PIM register messages for this (S, G) route.
SR - Sending Registers	Flag that indicates that the first-hop DR has begun sending registers for this (S, G) route, but has not yet received a Register-Stop message.
E - MSDP External	Flag that is set on those entries that have sources, learned through Multicast Source Discovery Protocol (MSDP), from another RP.
ME - MDT Encap	Flag that indicates a core encapsulation route for a multicast distribution tree (MDT).
MD - MDT Decap	Flag that indicates a core decapsulation route for an MDT.
MT - Crossed Data MDT threshold	Flag that indicates that traffic on this route passed a threshold for the data MDT.
MA - Data MDT group assigned	Flag that indicates a core encapsulation route for the data MDT.
POS0/2/0/0	Interface name. Name of an interface in the interface list of the entry.

Field	Description
03:54:23	Interface uptime. Time (in hours, minutes, and seconds) this interface has existed in the entry.
off	Interface forwarding status. Outgoing forwarding status of the interface for the entry is “fwd” or “off”.
Interface Information Flags	
LI - Local Interest	Flag that indicates that there are local receivers for this entry on this interface, as reported by Internet Group Management Protocol (IGMP).
LD - Local Disinterest	Flag that indicates that there is explicit disinterest for this entry on this interface, as reported by IGMP exclude mode reports.
II - Internal Interest	Flag that indicates that the host stack of the router has internal receivers for this entry.
ID - Internal Disinterest	Flag that indicates that the host stack of the router has explicit internal disinterest for this entry.
LH - Last Hop	Flag that indicates that this interface has directly connected receivers and this router serves as a last hop for the entry. If the (S, G) outgoing interface list is inherited from a (*, G) route, the LH flag is set on the (*, G) outgoing LH interface.
AS - Assert	Flag that indicates that a PIM assert message was seen on this interface and the active PIM assert state exists.
AB - Administrative Boundary	Flag that indicates that forwarding on this interface is blocked by a configured administrative boundary for this entry’s group range.

Related Commands

Command	Description
show mfib route	Displays all entries in the MFIB table.

show pim topology detail

To display detailed Protocol Independent Multicast (PIM) routing topology information that includes references to the tables in which reverse path forwarding (RPF) lookups occurred for specific topology route entries, use the **show pim topology detail** command in

EXEC

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **topology detail**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

When the multicast-only fast reroute (MoFRR) feature is enabled, the **show pim topology detail** command shows the primary and secondary paths for SGs configured for MoFRR.

Note For forwarding information, use the **show mfib route** and **show mrib route** commands.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim topology detail** command, showing the RPF table information for each topology entry:

```
RP/0/# show pim ipv4 topology detail

IP PIM Multicast Topology Table:
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected,
    ME - MDT Encap, MD - MDT Decap,
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary


(*,224.0.1.40) DM Up: 00:07:28 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
RPF Table: None
  GigabitEthernet0/1/0/1      00:07:28  off LI II LH
  GigabitEthernet0/1/0/2      00:07:23  off LI LH
  GigabitEthernet0/1/0/1.503  00:07:27  off LI LH

(11.11.11.11,232.5.0.2)SPT SSM Up: 00:07:21
JP: Join(now) RPF: GigabitEthernet0/1/0/1.203,11.23.0.20 Flags:
RPF Table: IPv4-Unicast-default
  GigabitEthernet0/1/0/1.501  00:07:21  fwd LI LH

(61.61.0.10,232.5.0.3)SPT SSM Up: 00:11:57
JP: Join(now) RPF: Null,0.0.0.0 Flags:
RPF Table: None (Dropped due to route-policy)
  No interfaces in immediate olist
```

Note The RPF table output in boldface indicates the table in which the RPF lookup occurred for this route entry.

The following example shows output for a MoFRR convergence:

```
RP/0/# show pim topology 239.1.1.1 detail

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected,
    ME - MDT Encap, MD - MDT Decap,
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1)SPT SSM Up: 13:54:06
JP: Join(00:00:41) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
  GigabitEthernet0/5/0/1      13:54:06  fwd LI LH
RP/0/4/CPU0:Sunnyvale#show pim topology 239.1.1.1 detail

IP PIM Multicast Topology Table
```

```
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected,
    ME - MDT Encap, MD - MDT Decap,
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1)SPT SSM Up: 13:54:10
JP: Join(00:00:37) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/5/0/3.2,100.100.200.10
  GigabitEthernet0/5/0/1      13:54:10  fwd LI LH
```

show pim topology, on page 182 describes the significant fields shown in the display , including those related to multicast-only fast reroute (MoFRR) . This table includes fields that do not appear in the example, but that may appear in your output.

Related Commands

Command	Description
show mfib route	Displays all entries in the MFIB table.
show mrib route	Displays all entries in the MRIB table.

show pim topology entry-flag

To display Protocol Independent Multicast (PIM) routing topology information for a specific entry flag, use the **show pim topology entry-flag** command in

EXEC

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **topology entry-flag** *flag* [**detail** | **route-count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
flag	Configures a display of routes with the specified entry flag. Valid flags are the following: • **AA** —Assume alive • **DCC** —Don't check connected • **DSS** —Don't signal sources • **E** —MSDP External • **EX** —Extranet flag set • **IA** —Inherit except flag set • **KAT** —Keepalive timer • **LH** —Last hop • **PA** —Probe alive • **RA** —Really alive • **RR** —Registered receiver • **SR** —Sending registers
detail	(Optional) Specifies details about the entry flag information.
route-count	(Optional) Displays the number of routes in the PIM topology table.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** and **show mrib route** commands.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim topology entry-flag** command:

```
RP/0/# show pim topology entry-flag E

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources,  RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(202.5.5.202,226.0.0.0)SPT SM Up: 00:27:06
JP: Join(00:00:11) RPF: GigabitEthernet0/2/0/2,44.44.44.103 Flags: KAT(00:01:54) E RA
  No interfaces in immediate olist

(203.5.5.203,226.0.0.0)SPT SM Up: 00:27:06
JP: Join(00:00:11) RPF: GigabitEthernet0/2/0/2,44.44.44.103 Flags: KAT(00:01:54) E RA
  No interfaces in immediate olist

(204.5.5.204,226.0.0.0)SPT SM Up: 00:27:06
JP: Join(00:00:11) RPF: GigabitEthernet0/2/0/2,44.44.44.103 Flags: KAT(00:01:54) E RA
  No interfaces in immediate olist

(204.5.5.204,226.0.0.1)SPT SM Up: 00:27:06
JP: Join(00:00:11) RPF: GigabitEthernet0/2/0/2,44.44.44.103 Flags: KAT(00:01:54) E RA
  No interfaces in immediate olist
```

show pim topology, on page 182 describes the significant fields shown in the display. This table includes fields that do not appear in the example, but that may appear in your output.

Related Commands

Command	Description
show mrib route	Displays all entries in the MRIB table.

show pim topology interface-flag

To display Protocol Independent Multicast (PIM) routing topology information for a specific interface, use the **show pim topology** command in

EXEC
mode

.

show pim [**vrf** *vrf-name*] [**ipv4**] **topology interface-flag** *flag* [**detail** | **route-count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
flag	Configures a display of routes with the specified interface flag. Valid flags are the following:
detail	(Optional) Displays details about the interface flag information.
route-count	(Optional) Displays the number of routes in the PIM topology table.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** and **show mrib route** commands.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim topology interface-flag** command:

```
RP/0/# show pim topology interface-flag LI

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources,  RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(*,224.0.1.39) DM Up: 00:27:27 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
  Loopback5                   00:27:27  off LI II LH

(*,224.0.1.40) DM Up: 00:27:27 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
  Loopback5                   00:27:26  off LI II LH
  GigabitEthernet0/2/0/2      00:27:27  off LI LH

(*,226.0.0.0) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
  Loopback5                   00:27:27  fwd LI LH

(*,226.0.0.1) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
  Loopback5                   00:27:27  fwd LI LH

(*,226.0.0.3) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
  Loopback5                   00:27:27  fwd LI LH

(*,226.0.0.4) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
  Loopback5                   00:27:27  fwd LI LH

(*,226.0.0.5) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
  Loopback5                   00:27:27  fwd LI LH

(201.5.5.201,226.1.0.0)SPT SM Up: 00:27:27
JP: Join(never) RPF: Loopback5,201.5.5.201* Flags: KAT(00:00:34) RA RR (00:03:53)
  GigabitEthernet0/2/0/2      00:26:51  fwd Join(00:03:14)
  Loopback5                   00:27:27  fwd LI LH

(204.5.5.204,226.1.0.0)SPT SM Up: 00:27:27
JP: Join(now) RPF: GigabitEthernet0/2/0/2,44.44.44.103 Flags: E
  Loopback5                   00:27:27  fwd LI LH
```

show pim topology, on page 182 describes the significant fields shown in the display. This table includes fields that do not appear in the example, but that may appear in your output.

Related Commands

Command	Description
show mrib route	Displays all entries in the MRIB table.

show pim topology summary

To display summary information about the Protocol Independent Multicast (PIM) routing topology table, use the **show pim topology summary** command in

EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**] **topology summary** [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
detail	(Optional) Displays details about the summary information.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** and **show mrib route** commands.

Task ID

Task ID	Operations
multicast	read

Examples

The following example represents sample output from the **show pim topology summary** command:

```
RP/0/# show pim vrf svpn12 topology summary
```

```
Mon Feb  2 04:07:01.249 UTC
PIM TT Summary for VRF svpn12
  No. of group ranges = 9
  No. of (*,G) routes = 8
  No. of (S,G) routes = 2
  No. of (S,G)RPT routes = 0

OSPF Mcast-intact   Not configured
    ISIS Mcast-intact   Not configured
    ISIS Mcast Topology Not configured

Default RPF Table: IPv4-Unicast-default
RIB Convergence Timeout Value: 00:30:00
RIB Convergence Time Left:     00:28:32
Multipath RPF Selection is Enabled

Table: IPv4-Unicast-default
    PIM RPF Registrations = 13
    RIB Table converged

Table: IPv4-Multicast-default
    PIM RPF Registrations = 0
    RIB Table converged
```

For an example of detailed PIM topology output, see show pim topology detail, on page 188.

show pim traffic

To display Protocol Independent Multicast (PIM) traffic counter information, use the **show pim traffic** command in EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim traffic** command that displays a row for valid PIM packets, number of hello packets, and so on:

```
RP/0/# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 1d01h

                  Received                       Sent
Valid PIM Packets 15759217                    15214426
Hello                9207                       12336
Join-Prune        1076805                      531981
Data Register    14673205                           0
Null Register       73205                           0
Register Stop           0                    14673205
Assert                  0                           0
Batched Assert          0                           0
BSR Message             0                           0
Candidate-RP Adv.       0                           0

Join groups sent                                    0
Prune groups sent                                   0
Output JP bytes                                     0
Output hello bytes                               4104
```

```
Errors:
Malformed Packets                                   0
Bad Checksums                                       0
Socket Errors                                       0
Subnet Errors                                       0
Packets dropped since send queue was full           0
Packets dropped due to invalid socket               0
Packets which couldn't be accessed                  0
Packets sent on Loopback Errors                     6
Packets received on PIM-disabled Interface          0
Packets received with Unknown PIM Version           0
```

This table describes the significant fields shown in the display.

Table 32: show pim traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Time (in days and hours) that had elapsed since the counters were cleared with the **clear pim counters** command.
Valid PIM Packets	Total PIM packets that were received and sent.
HelloJoin-PruneRegisterRegister StopAssert Bidir DF Election	Specific type of PIM packets that were received and sent.
Malformed Packets	Invalid packets due to format errors that were received and sent.
Bad Checksums	Packets received or sent due to invalid checksums.
Socket Errors	Packets received or sent due to errors from the router's IP host stack sockets.
Packets dropped due to invalid socket	Packets received or sent due to invalid sockets in the router's IP host stack.
Packets which couldn't be accessed	Packets received or sent due to errors when accessing packet memory.
Packets sent on Loopback Errors	Packets received or sent due to use of loopback interfaces.
Packets received on PIM-disabled Interface	Packets received or sent due to use of interfaces not enabled for PIM.
Packets received with Unknown PIM Version	Packets received or sent due to invalid PIM version numbers in the packet header.

Related Commands

Command	Description
clear pim counters, on page 102	Clears Protocol Independent Multicast (PIM) counters and statistics.

show pim tunnel info

To display information for the Protocol Independent Multicast (PIM) tunnel interface, use the **show pim tunnel info** command in

EXEC mode

mode.

show pim [**vrf** *vrf-name*] [**ipv4**] **tunnel info** {*interface-unit* | **all**} [**netio**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
interface-unit	Name of virtual tunnel interface that represents the encapsulation tunnel or the decapsulation tunnel.
all	Specifies both encapsulation and decapsulation tunnel interfaces.
netio	(Optional) Displays information obtained from the Netio DLL.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

PIM register packets are sent through the virtual encapsulation tunnel interface from the source's first-hop designated router (DR) router to the rendezvous point (RP). On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to sparse mode (SM), not to Source Specific Multicast (SSM) .

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim tunnel info** command:

```
RP/0/# show pim tunnel info all

Interface         RP Address      Source Address
Encapstunnel0     10.1.1.1        10.1.1.1
Decapstunnel0     10.1.1.1
```

This table describes the significant fields shown in the display.

Table 33: show pim tunnel info Field Descriptions

Field	Description
Interface	Name of the tunnel interface.
RP Address	IP address of the RP tunnel endpoint.
Source Address	IP address of the first-hop DR tunnel endpoint, applicable only to encapsulation interfaces.

show pim vrf vrf_name rpf

To display RPF information for protocol independent multicast, use the **show pim vrf** *vrf1* **rpf** command in the EXEC mode.

show pim vrf *vrf1* **rpf**

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read

```
RP/0/# show pim vrf vrf1 rpf
Table: IPv4-Unicast-default
* 192.1.1.2/32 [200/0]
    via MPLS  with rpf neighbor 110.110.110.110
    Connector: 1:1:110.110.110.110, Nexthop: 110.110.110.110
```

show pim vrf vrf_name topology

To display the PIM topology table information for a specific vrf, use the **show pim vrf** *vrf_name* **topology** command in the EXEC mode.

show pim vrf *vrf_name* **topology** *ip_address*

Syntax Description

ip_address	Specifies the IP address.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read

```
RP/0/# show pim vrf vrf1 topology 232.1.1.1

(192.1.1.2,232.1.1.1)SPT SSM Up: 05:53:44
JP: Join(00:00:09) RPF: GigabitEthernet0/0/0/1.1,192.1.1.2* Flags: MT
  tunnel-mte1                 05:53:44  fwd LI LH
```

spt-threshold infinity

To change the behavior of the last-hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the **spt-threshold infinity** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

spt-threshold infinity [**group-list** *access-list*]
no spt-threshold infinity

Syntax Description

group-list *access-list*	(Optional) Indicates the groups restricted by the access list.

Command Default

The last-hop Protocol Independent Multicast (PIM) router switches to the shortest-path source tree by default.

Command Modes

PIM configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **spt-threshold infinity** command causes the last-hop PIM router to always use the shared tree instead of switching to the shortest-path source tree.

If the **group-list** keyword is not used, this command applies to all multicast groups.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the PIM source group grp1 to always use the shared tree:

```
RP/0/(config)# router pim
RP/0/(config-pim-default-ipv4)# spt-threshold infinity group-list grp1
```

ssm

To define the Protocol Independent Multicast (PIM)-Source Specific Multicast (SSM) range of IP multicast addresses, use the **ssm** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

ssm [**allow-override** | **disable** | **range** *access-list*]
no ssm [**allow-override** | **disable** | **range**]

Syntax Description

allow-override	(Optional) Allows SSM ranges to be overridden by more specific ranges.
disable	(Optional) Disables SSM group ranges.
range *access-list*	(Optional) Specifies an access list describing group ranges for this router when operating in PIM SSM mode.

Command Default

Interface operates in PIM sparse mode (PIM-SM). IPv4 addressing is the default.

Command Modes

Multicast routing configuration

Multicast routing address-family configuration

Multicast VPN configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ssm** command performs source filtering, which is the ability of a router to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address. Unlike PIM-sparse mode (SM) that uses a rendezvous point (RP) and shared trees, PIM-SSM uses information on source addresses for a multicast group provided by receivers through the local membership protocol Internet Group Management Protocol (IGMP) and is used to directly build source-specific trees.

IGMP Version 3 must be enabled on routers that want to control the sources they receive through the network.

When multicast routing is enabled, the default is PIM-SSM enabled on the default SSM range, 232/8. SSM may be disabled with the **disable** form of the command, or any ranges may be specified in an access list with the **range** form. All forms of this command are mutually exclusive. If an access list is specified, the default SSM range is not used unless specified in the access list.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure SSM service for the IP address range defined by access list 4, using the **ssm** command:

```
RP/0/(config)# ipv4 access-list 4
RP/0/(config-ipv4-acl)# permit ipv4 any 224.2.151.141
RP/0/(config)# multicast-routing
RP/0/(config-mcast)# ssm range 4
```



Multicast Routing Forwarding Commands

- accounting per-prefix, on page 209
- address-family (multicast), on page 211
- clear mfib counter, on page 214
- clear mfib database, on page 215
- clear mfib platform, on page 216
- disable (multicast), on page 218
- enable (multicast), on page 220
- forwarding-latency, on page 222
- hw-module route-stats , on page 223
- hw-module multicast route-scale, on page 225
- interface-inheritance disable, on page 226
- interface all enable, on page 228
- interface (multicast), on page 230
- log-traps, on page 232
- maximum disable, on page 233
- mdt data ingress replication, on page 234
- mdt default ingress replication, on page 235
- mdt partitioned ingress replication, on page 236
- migration route-policy, on page 237
- multicast-routing, on page 238
- multipath, on page 239
- nsf (multicast) , on page 241
- oom-handling, on page 243
- rate-per-route, on page 244
- route-policy, on page 245
- shared-tree-prune delay, on page 246
- show mfib connections, on page 247
- show mfib counter, on page 249
- show mfib encap-info , on page 251
- show mfib interface, on page 252
- show mfib nsf, on page 254
- show mfib platform route, on page 256
- show mfib route, on page 260

- show mfib table-info, on page 262
- show mrib client, on page 264
- show mrib mpls forwarding, on page 267
- show mrib mpls route, on page 269
- show mrib nsf, on page 270
- show mrib nsr end, on page 272
- show mrib route-collapse, on page 274
- show mrib route, on page 276
- show mrib route outgoing-interface, on page 279
- show mrib table-info, on page 281
- show mrib tlc, on page 283
- show mrib vrf vrf_name route, on page 284
- source-tree-prune-delay, on page 285
- static-rpf, on page 286
- suppress-pim-data-signaling, on page 288
- suppress-shared-tree-join, on page 289
- unicast-reachability, on page 290
- vrf (multicast), on page 291

accounting per-prefix

To enable accounting for multicast routing, use the **accounting per-prefix** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

accounting per-prefix
no accounting per-prefix

Syntax Description

This command has no keywords or arguments.

Command Default

This feature is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address family IPv4 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **accounting per-prefix** command is used to enable per-prefix counters only in hardware. Cisco IOS XR Software counters are always present. When enabled, IPv4 (S,G) routes with a /32 prefix and IPv6 (S,G) routes with a /128 prefix are assigned a single forwarding counter.

There are a limited number of counters on all nodes. When a command is enabled, counters are assigned to routes only if they are available.

To display packet statistics, use the **show mfib route statistics location** command. These commands display `N/A` for hardware forwarding counts when there are no hardware statistics available or when the **accounting per-prefix** command is disabled.

To view MFIB accounting and per-route rates, configure both **rate-per-route** and **accounting per-prefix** under multicast-routing address-family.

To enable statistics for routes in a VRF, configure **rate-per-route** and **accounting per-prefix** under the corresponding multicast-routing VRF address family.

If there are limited number of counters available and you want to enable counters on particular prefixes for troubleshooting purposes, you can configure **hw-module route-stats** to enable accounting for multicast routing for a limited number of routes.

For more information, see the hw-module route-stats , on page 223 command to configure a filter to choose which (S.G) routes will have statistics enabled.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable accounting for multicast routing:

```
Router(config)# multicast-routing
Router(config-mcast)# address-family ipv4
Router(config-mcast-default-ipv4)# rate-per-route
Router(config-mcast-default-ipv4)# accounting per-prefix
```

Related Commands

Command	Description
show mfib route, on page 260	Displays route entries in the Multicast Forwarding Information Base (MFIB).
hw-module route-stats , on page 223	To configure multicast per-route statistics.

address-family (multicast)

To display available IP prefixes to enable multicast routing and forwarding on all router interfaces, use the **address-family** command in multicast-routing configuration mode or multicast VRF configuration submode. To disable use of an IP address prefix for routing, use the **no** form of this command.

address-family [**vrf** *vrf-name*] {**ipv4** | **ipv6**}
no address-family [**vrf** *vrf-name*] {**ipv4** | **ipv6**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.

Command Default

No default behavior or values

Command Modes

Multicast routing configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **address-family** command either from multicast routing configuration mode or from multicast VRF configuration sub to enter either the multicast IPv4 or IPv6 address family configuration submode, depending on which keyword was chosen. Use the **address-family** command with the multicast-routing, on page 238command to start the following multicast processes:

- Multicast Routing Information Base (MRIB)
- Multicast Forwarding Engine (MFWD)
- Protocol Independent Multicast Sparse mode (PIM-SM)
- Internet Group Management Protocol (IGMP)
- Multicast Listener Discovery Protocol (MLD)

Basic multicast services start automatically when the multicast PIE is installed, without any explicit configuration required. The following multicast services are started automatically:

- Multicast Routing Information Base (MRIB)
- Multicast Forwarding Engine (MFWD)
- Protocol Independent Multicast Sparse mode (PIM-SM)
- Internet Group Management Protocol (IGMP)

Other multicast services require explicit configuration before they start. For example, to start the Multicast Source Discovery Protocol (MSDP) process, you must enter the **router msdp** command and explicitly configure it.

To enable multicast routing and protocols on interfaces, you must explicitly enable the interfaces using the **interface** command in multicast routing configuration mode. This action can be performed on individual interfaces or by configuring a wildcard interface using the **alias** command.

To enable multicast routing on all interfaces, use the **interface all enable** command in multicast routing configuration mode. For any interface to be fully enabled for multicast routing, it must be enabled specifically (or configured through the **interface all enable** command for all interfaces) in multicast routing configuration mode, and it must not be disabled in the PIM and IGMP configuration modes.

Note The **enable** and **disable** keywords available under the IGMP and PIM interface configuration modes have no effect unless the interface is enabled in multicast routing configuration mode—either by default or by explicit interface configuration.

To allow multicast forwarding functionality, while turning multicast routing functionality off, interface-inheritance disable, on page 226command on a per interface or **interface all enable** basis in PIM or IGMP configuration mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

This example shows how to enter IPv4 and IPv6 multicast routing configuration mode:

```
Router(config)# multicast-routing
Router(config-mcast)# address-family ipv4
Router(config-mcast-default-ipv4)#

Router(config-mcast)# address-family ipv6
Router(config-mcast-default-ipv6)#
```

This example shows how to enter IPv4 and IPv6 VRF multicast routing configuration submode:

```
Router(config)# multicast-routing
Router(config-mcast)# vrf vrf-name address-family ipv4
Router(config-mcast-vrf-name-ipv4)#

Router(config-mcast)# vrf vrf-name address-family ipv6

-
```

Related Commands

Command	Description
alias	Creates a command alias.
interface all enable, on page 228	Enables multicast routing and forwarding on all new and existing interfaces.
interface all disable	Disables PIM processing on all new and existing interfaces.
interface-inheritance disable, on page 226	Separates the disabling of multicast routing and forwarding.

Command	Description
interface (multicast), on page 230	Configures multicast interface properties.

clear mfib counter

To clear Multicast Forwarding Information Base (MFIB) route software counters, use the **clear mfib counter** command in the appropriate mode.

clear mfib [**vrf** *vrf-name*] **ipv4 counter** [*group-addresssource-address*] [**location** {*node-id* | **all**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
group-address	(Optional) IP address of the multicast group.
source-address	(Optional) IP address of the source of the multicast route.
location *node-id*	(Optional) Clears route packet counters from the designated node.
all	The **all** keyword clears route packet counters on all nodes

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Note This command only clears MFIB route packet software counters.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to clear MFIB software counters on all nodes:

```
Router# clear mfib counter location all
```

clear mfib database

To clear the Multicast Forwarding Information Base (MFIB) database, use the **clear mfib database** command in the appropriate mode.

clear mfib [**ipv4** | **ipv6**] **database**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The clear mfib database location <**node-id** | **all**> command is not supported on Cisco 8000 Series Routers.



Caution Executing clear mfib database can trigger a line card or router reload, depending on the location from which the command is executed.

Task ID

Task ID	Operations
multicast	read, write, execute

clear mfib platform

To clear Multicast Forwarding Information Base (MFIB) route hardware packet counters, use the **clear mfib platform** command in the appropriate mode.

clear mfib [**vrf** *vrf-name*] [**ipv4** | **ipv6**] **platform route statsistics** [*group-address source-address*] [**location** { *node-id* | **all** }]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
group-address	(Optional) IP address of the multicast group.
source-address	(Optional) IP address of the source of the multicast route.
location *node-id*	(Optional) Clears route packet counters from the designated node.
all	The **all** keyword clears route packet counters on all nodes

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

Note To clear ingress statistics of a route, you can get the `stats-ole` location for a specified route using the **show mrib route detail** command.

A `stats-ole` is a counter that is programmed on one of the line cards in the system for a particular route. This counter helps report ingress statistics for the route.

If you do not know the `stats-ole` location, you can use the option **location all** instead, which helps to find the specific `stats-ole` location and clear the ingress counters.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to clear the ingress statistics for a route if `stats-ole` location is known:

```
Router# clear mfib platform route statistics location 0/11/CPU0
```

disable (multicast)

To disable multicast routing and forwarding on an interface, use the **disable** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

disable
no disable

Syntax Description

This command has no keywords or arguments.

Command Default

Multicast routing and forwarding settings are inherited from the global **interface enable all** command. Otherwise, multicast routing and forwarding is disabled.

Command Modes

Multicast routing interface configuration

Multicast routing VRF interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **disable** command modifies the behavior of a specific interface to disabled. This command is useful if you want to disable multicast routing on specific interfaces, but leave it enabled on all remaining interfaces.

The following guidelines apply when the **enable** and **disable** commands (and the **no** forms) are used in conjunction with the **interface all enable** command:

- If the **interface all enable** command is configured:
  - The **enable** and **no** forms of the command have no additional effect on a specific interface.
  - The **disable** command disables multicast routing on a specific interface.
  - The **no disable** command enables a previously disabled interface.
- If the **interface all enable** command is not configured:
  - The **enable** command enables multicast routing on a specific interface.
  - The **no enable** command enables the previously disabled interface.
  - The **disable** and **no** forms of the command have no additional effect on a specific interface.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable multicast routing on all interfaces and disable the feature only on GigabitEthernet interface 0/1/0/0:

```
Router(config)# multicast-routing
Router(config-mcast)# interface all enable
Router(config-mcast-default-ipv4)# interface HundredGigE 0/0/0/24
Router(config-mcast-default-ipv4-if)# disable
```

Related Commands

Command	Description
enable (multicast), on page 220	Enables multicast routing and forwarding on an interface.
interface all enable, on page 228	Enables multicast routing and forwarding on all new and existing interfaces.

enable (multicast)

To enable multicast routing and forwarding on an interface, use the **enable** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

enable
no enable

Syntax Description

This command has no keywords or arguments.

Command Default

Multicast routing and forwarding settings are inherited from the global **interface enable all** command. Otherwise, multicast routing and forwarding is disabled.

Command Modes

Multicast routing interface configuration

Multicast routing VRF interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **enable** command modifies the behavior of a specific interface to enabled. This command is useful if you want to enable multicast routing on specific interfaces, but leave it disabled on all remaining interfaces.

The following guidelines apply when the **enable** and **disable** commands (and the **no** forms) are used in conjunction with the **interface all enable** command:

- If the **interface all enable** command is configured:
  - The **enable** and **no** forms of the command have no additional effect on a specific interface.
  - The **disable** command disables multicast routing on a specific interface.
  - The **no disable** command enables a previously disabled interface.
- If the **interface all enable** command is not configured:
  - The **enable** command enables multicast routing on a specific interface.
  - The **no enable** command enables a previously enabled interface.
  - The **disable** and **no** forms of the command have no additional effect on a specific interface.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable multicast routing on a specific interface only:

```
Router(config)# multicast-routing
Router(config-mcast)# interface HundredGigE 0/0/0/24
Router(config-mcast-default-ipv4-if)# enable
```

Related Commands

Command	Description
disable (multicast), on page 218	Disables multicast routing and forwarding on an interface.
interface all enable, on page 228	Enables multicast routing and forwarding on all new and existing interfaces.

forwarding-latency

To delay traffic being forwarded on a route, use the **forwarding-latency** command. To return to the default behavior, use the **no** form of this command.

forwarding-latency [**delay** *milliseconds*]
no forwarding-latency

Syntax Description

delay *milliseconds*	(Optional) Specifies the delay time in miliseconds. Range is 5 - 500.

Command Default

The default delay time is 30 milliseconds.

Command Modes

Multicast routing configuration

IPv4 and IPv6 multicast routing configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **forwarding-latency** command when you expect a receiver to leave and rejoin the same multicast group within a very short period such as 20 or 30 milliseconds. The delay may be required to provide the router sufficient time to update its Multicast Forwarding Information Base (MFIB) table.

When the **forwarding-latency** command is enabled, each interface is allocated a separate table lookup unit (TLU) block in the output interface list (olist), thereby increasing TLU hardware resource usage, and, for this reason, it should be used with caution when many multicast routes are present.

When the **forwarding-latency** command is disabled, up to three interfaces may share a single TLU block in the olist.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to delay traffic from being forwarded for 120 milliseconds:

```
RP/0/# configure
RP/0/(config)# multicast-routing
RP/0/# forwarding-latency delay 120
```

hw-module route-stats

To configure multicast per-route statistics, use the **hw-module route-stats** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

hw-module route-stats l3mcast [**vrf** *vrf-name*] {**ipv4** | **ipv6**} *access-list*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4 *access-list*	(Optional) Specifies IPv4 access-list.
ipv6 *access-list*	(Optional) Specifies IPv6 access-list.

Command Default

This feature is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

You need to configure **accounting-per-prefix** under multicast-routing mode to enable accounting for the routes. If the number of multicast routes exceeds the available statistics, for troubleshooting purposes, you can use the **hw-module route-stats** command to apply a filter on which specific (S,G) routes will have allocated statistics counters.

(S,G) routes that match the access-list used in the configuration will have statistics enabled, and other routes will not. There is no need to reload the router or reload the line card for the filter to take effect.

To reassign statistics to different (S,G) you need to remove the **accounting-per-prefix** and **hw-module route-stats** configurations, modify the access-list and reapply the configuration again.

Note The **hw-module route-stats** command should only be used in conjunction with the **accounting-per-prefix** configuration.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable accounting for multicast routing:

```
Router(config)# ipv4 access-list mcast-counter
Router(config-acl)# 10 permit ipv4 host 10.1.1.2 host 224.2.151.1
Router(config-acl)# 30 permit ipv4 10.1.1.0/24 232.0.4.0/22
Router(config-acl)# 50 permit ipv4 192.168.0.0/24 232.0.4.0/22
Router(config-acl)#commit
```

```
Router(config-acl)#exit
Router(config)# hw-module route-stats l3mcast vrf default ipv4 mcast-counter
```

Related Commands

Command	Description
accounting per-prefix, on page 209	Enables accounting for multicast routing.

hw-module multicast route-scale

To enable the 120k scale for IPv4 Source Specific Multicast (SSM), use the **hw-module multicast route-scale** command in the . To remove the configuration, use the **no** form of this command.

hw-module multicast route-scale

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.3.15	This command was introduced.

Usage Guidelines

This command is applicable only for IPv4 SSM. IPv6 supports 64K routes.

This command is supported only on modular systems and not on fixed/centralized systems.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable the 120K scale for IPv4 SSM:

```
Router# configure
Router(config)# hw-module multicast route-scale
```

interface-inheritance disable

To separate PIM and IGMP routing from multicast forwarding on all interfaces, use the **interface-inheritance disable** command under multicast routing address-family IPv4 submode. To restore the default functionality, use the **no** form of the command.

interface-inheritance disable
no interface-inheritance disable

Syntax Description

This command has no keywords or arguments.

Command Default

This feature is not enabled by default.

Command Modes

Multicast routing configuration

Address- family IPv4 configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use of the **interface-inheritance disable** command together with the **interface** *type interface-path-id* or **interface all enable** command under multicast routing address-family IPv4 submode separates PIM and IGMP routing functionality from multicast forwarding on specified interfaces. You can nonetheless enable multicast routing functionality explicitly under PIM or IGMP routing configuration mode for individual interfaces.



Note Although you can explicitly configure multicast routing functionality on individual interfaces, you cannot explicitly disable the functionality. You can only disable the functionality on all interfaces.

Used from the address-family ipv4 configuration submode, it prevents IGMP and PIM from inheriting the multicast-routing interface configuration.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following configuration disables PIM and IGMP routing functionality on all the interfaces using the **interface-inheritance disable** command, but multicast forwarding is still enabled on all the interfaces in the example, based on use of the keywords **interface all enable** .

PIM is enabled on *Loopback 0* based on its explicit configuration (**interface** *Loopback0* **enable**) under router pim configuration mode.

IGMP protocol is enabled on GigabitEthernet0/6/0/3, because it too has been configured explicitly under router igmp configuration mode (**interface** *GigabitEthernet0/6/0/3* **router enable**):

```
RP/0/(config)# multicast-routing
RP/0/(config-mcast)# address-family ipv4
RP/0/(config-mcast-default-ipv4)# interface-inheritance disable
RP/0/(config-mcast-default-ipv4)# interface loopback 1 enable

RP/0/(config-mcast-default-ipv4)# show run router pim
```

With the **interface-inheritance disable** command in use, IGMP and PIM configuration are enabled in the protocol configuration as follows:

```
router igmp
  interface loopback 0
    router enable

router pim
   interface loopback 0
     enable

router pim vrf default address-family ipv4
 interface Loopback0
  enable


RP/0/(config-mcast-default-ipv4)# show run router igmp

router igmp
 vrf default
  interface GigabitEthernet0/6/0/3
   router enable
```

interface all enable

To enable multicast routing and forwarding on all new and existing interfaces, use the **interface all enable** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

interface all enable
no interface all enable

Syntax Description

This command has no keywords or arguments.

Command Default

Multicast routing and forwarding is disabled by default.

Command Modes

Multicast routing configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command modifies the default behavior for all new and existing interfaces to enabled unless overridden by the **enable** or **disable** keywords available in interface configuration mode.

The following guidelines apply when the **enable** and **disable** commands (and the **no** forms) are used in conjunction with the **interface all enable** command:

- If the **interface all enable** command is configured:
  - The **enable** and **no** forms of the command have no additional effect on a specific interface.
  - The **disable** command disables multicast routing on a specific interface.
  - The **no disable** command enables a previously disabled interface.
- If the **interface all enable** command is not configured:
  - The **enable** command enables multicast routing on a specific interface.
  - The **no enable** command enables a previously enabled interface.
  - The **disable** and **no** forms of the command have no additional effect on a specific interface.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable multicast routing on all interfaces and disable the feature only on GigabitEthernet interface 0/1/0/0:

```
Router(config)# multicast-routing
Router(config-mcast)# interface all enable
Router(config-mcast)# interface HundredGigE 0/0/0/24
Router(config-mcast-default-ipv4-if)# disable
```

Related Commands

Command	Description
disable (multicast), on page 218	Disables multicast routing and forwarding on an interface.
enable (multicast), on page 220	Enables multicast routing and forwarding on an interface.

interface (multicast)

To configure multicast interface properties, use the **interface** command in the appropriate configuration mode. To disable multicast routing for interfaces, use the **no** form of this command.

interface *type interface-path-id*
no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

Multicast routing configuration

IPv4 or multicast routing configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **interface** command to configure multicast routing properties for specific interfaces.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable multicast routing on all interfaces and disable the feature only on GigabitEthernet interface 0/1/0/0:

```
Router(config)# multicast-routing
Router(config-mcast)# interface all enable
```

```
Router(config-mcast-default-ipv4-if)# interface HundredGigE 0/0/0/24
Router(config-mcast-default-ipv4-if)# disable
```

Related Commands

Command	Description
disable (multicast), on page 218	Disables multicast routing and forwarding on an interface.
enable (multicast), on page 220	Enables multicast routing and forwarding on an interface.
interface all enable, on page 228	Enables multicast routing and forwarding on all new and existing interfaces.

log-traps

To enable logging of trap events, use the **log-traps** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

log-traps
no log-traps

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address family IPv4 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable logging of trap events:

```
RP/0/# multicast-routing
RP/0/(config-mcast)# log-traps
```

maximum disable

To disable maximum state limits, use the **maximum disable** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

maximum disable
no maximum disable

Syntax Description

This command has no keywords or arguments.

Command Default

Maximum state limits are enabled.

Command Modes

Multicast routing configuration

Multicast routing address family IPv4 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **maximum disable** command to override the default software limit on the number of multicast routes.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to disable maximum state limits:

```
RP/0/# multicast-routing
RP/0/(config-mcast)# maximum disable
```

mdt data ingress replication

To configure ingress replication (IR) data for Multicast Distribution Trees (MDT), use the **mdt data ingress replication** command in the appropriate mode. To remove the configuration, use the **no** form of the command.

mdt data ingress replication [*acl-name* | **immediate switch** | **number** *value* | **route-policy** | **threshold** *value*]

Syntax Description

immediate switch	Enables switching to data MDT immediately.
acl-name	ACL for vrf groups that are enabled for data MDT
number*value*	Maximum number of data MDTs to be triggered. Range is 1 to 262143.
route policy	Data MDT route policy.
threshold*value*	Traffic rate threshold (in kbps) to trigger data MDT. Range is 1 to 4294967.

Command Default

None

Command Modes

Multicast routing VRF address-family configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure ingress replication by using the **mdt data ingress replication** command:

```
Router# multicast-routing
Router(config-mcast) # mdt data ingress-replication
```

mdt default ingress replication

To configure ingress replication (IR) default for Multicast Distribution Trees (MDT), use the **mdt default ingress replication** command in the appropriate mode. To remove the configuration, use the **no** form of the command.

mdt default ingress replication

This command has no keywords or arguments.

Command Default

None

Command Modes

Multicast routing VRF address-family configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the MDT default group address from multicast routing configuration mode:

```
Router# multicast-routing
Router(config-mcast) # mdt default ingress-replication
```

mdt partitioned ingress replication

To configure ingress replication (IR) partitioned for Multicast Distribution Trees (MDT), use the **mdt partitioned ingress replication** command in the appropriate mode. To remove the configuration, use the **no** form of the command.

mdt partitioned ingress replication

This command has no keywords or arguments.

Command Default

None

Command Modes

Multicast routing VRF address-family configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the MDT partitioned group address from multicast routing configuration mode:

```
Router# multicast-routing
Router(config-mcast) # mdt partitioned ingress-replication
```

migration route-policy

To support PIM And BGP c-multicast joins over the same or different MDTs, use the **migration route-policy**command in the appropriate mode. To disable the migration, use the **no**form of the command.

migration route-policy *policy-name*
nomigration route-policy *policy-name*

Syntax Description

policy-name	Name of the policy.

Command Default

None

Command Modes

C-multicast routing configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The policy name is used to match the upstream PEs (nexthop) and send joins through BGP or PIM.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **migration route-policy**command:

```
RP/0/ (config-pim-v1-ipv4-mdt-cmcast) # migration route-policy p1
```

multicast-routing

To enter multicast routing configuration mode, use the **multicast-routing** command in global

configuration mode. To return to the default behavior, use the **no** form of this command.

multicast-routing
no multicast-routing

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enter multicast routing configuration mode:

```
RP/0/(config)# multicast-routing
RP/0/(config-mcast)#
```

Related Commands

Command	Description
accounting per-prefix, on page 209	Enables per-prefix counters only in hardware.
alias	Creates a command alias.
interface (multicast), on page 230	Configures multicast interface properties.
interface all enable, on page 228	Enables multicast routing and forwarding on all new and existing interfaces.

multipath

To enable Protocol Independent Multicast (PIM) to divide the multicast load among several equal cost paths, use the **multipath** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

[**address-family ipv4**] **multipath** [**hash** {**source** | **source next-hop**}]
no multipath

Syntax Description

source	Enables source-based multipath hashing.
source-nexthop	(Optional) Enables source with next-hop hashing.

Command Default

This command is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address-family ipv4

Multicast VRF configuration

Note Effective with IOS XR release 6.1.2 and later versions, **multipath** command is available only under the PIM configuration mode and not supported under the multicast routing configuration mode.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

By default, equal-cost multipath (ECMP) paths are not load balanced. A single path from each unicast route is used for all multicast routes (which is the equivalent of the **no** form of the multipath command).

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable multipath functionality for IOS XR release versions prior to 6.1.2.

```
RP/0/(config)# multicast-routing
RP/0/(config-mcast)# multipath hash
```

Note Effective with IOS XR release 6.1.2 and later versions, the **multipath** command is available only under the PIM configuration mode and not supported under the multicast routing configuration mode.

This example shows how to enable multipath functionality for IOS XR release 6.1.2 and later versions.

```
RP/0/(config)# router pim
RP/0/(config-pim)# multipath hash
```

nsf (multicast)

To turn on the nonstop forwarding (NSF) capability for the multicast routing system, use the **nsf** command in multicast routing configuration mode. To turn off this function, use the **no** form of this command.

nsf [**lifetime** *seconds*]
no nsf [**lifetime**]

Syntax Description

lifetime *seconds*	(Optional) Specifies the maximum time (in seconds) for NSF mode. Range is 30 to 3600.

Command Default

This command is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address family ipv4 configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **nsf** command does not enable or disable the multicast routing system, but just the NSF capability for all the relevant components. When the **no** form of this command is used, the NSF configuration is returned to its default disabled state.

Enable multicast NSF when you require enhanced availability of multicast forwarding. When enabled, failures of the control-plane multicast routing components Multicast Routing Information Base (MRIB) or Protocol Independent Multicast (PIM) will not cause multicast forwarding to stop. When these components fail or communication with the control plane is otherwise disrupted, existing Multicast Forwarding Information Base (MFIB) entries continue to forward packets until either the control plane recovers or the MFIB NSF timeout expires.

Enable multicast NSF when you upgrade control-plane Cisco IOS XR Software packages so that the live upgrade process does not interrupt forwarding.

When the MFIB partner processes enter NSF mode, forwarding on stale (nonupdated) MFIB entries continues as the control-plane components attempt to recover gracefully. Successful NSF recovery is signaled to the Multicast Forwarding Engine (MFWD) partner processes by MRIB. MRIB remains in NSF mode until Internet Group Management Protocol (IGMP) has recovered state from the network and host stack *and* until PIM has recovered state from the network and IGMP. When both PIM and IGMP have recovered and fully updated the MRIB, MRIB signals the MFIBs that NSF is ending, and begins updating the stale MFIB entries. When all updates have been sent, the MFWD partner processes delete all remaining stale MFIB entries and returns to normal operation, ending the NSF mode. MFIB NSF timeout prior to the signal from MRIB may cause NSF to end, and thus forwarding to stop.

When forwarding is in NSF mode, multicast flows may continue longer than necessary when network conditions change due to multicast routing protocols, unicast routing protocol reachability information, or local sender and receiver changes. The MFWD partner processes halt forwarding on stale MFIB entries when the potential for a multicast loop is detected by receipt of incoming data on a forwarding interface for the matching MFIB entry.

Note For NSF to operate successfully in your multicast network, you must also enable NSF for the unicast protocols (such as Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF] and Border Gateway Protocol [BGP]) that PIM relies on for Reverse Path Forwarding (RPF) information. See the appropriate configuration modules to learn how to configure NSF for unicast protocols.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable NSF for the multicast routing system:

```
RP/0/(config)# multicast-routing
RP/0/(config-mcast)# nsf
```

Related Commands

Command	Description
nsf lifetime (IGMP)	Configures the maximum time for the NSF timeout value under IGMP.
nsf lifetime (PIM)	Configures the NSF timeout value for the PIM process.
show igmp nsf	Displays the state of NSF operation in IGMP.
show mfib nsf	Displays the state of NSF operation for the MFIB line cards.
show mrib nsf, on page 270	Displays the state of NSF operation in the MRIB.
show pim nsf	Displays the state of NSF operation for PIM.

oom-handling

To enable the out-of-memory (OOM) functionality on multicast routing software components, use the **oom-handling** command in multicast routing configuration mode. To remove this functionality, use the **no** form of this command.

oom-handling
no oom-handling

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address family ipv4 configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When the **oom-handling** command is enabled, and the router memory is low or in a warning state, the following states are not created:

- Protocol Independent Multicast (PIM) route states in response to PIM join and prune messages, and register messages
- Internet Group Management Protocol (IGMP) group states
- External Source-Active (SA) states in Multicast Source Discovery Protocol (MSDP)

Multicast routing **show** commands such as the **show pim topology** command indicate when the router is running low on memory and that new state creation has stopped.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable the out-of-memory functionality:

```
RP/0/# multicast-routing
RP/0/(config-mcast)# oom-handling
```

Related Commands

Command	Description
show pim topology	Displays PIM topology table information.

rate-per-route

To enable individual (source, group [S, G]) rate calculations, use the **rate-per-route** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

rate-per-route
no rate-per-route

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address family ipv4 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable individual route calculations:

```
RP/0/# multicast-routing vrf vpn12 address-family ipv4
RP/0/(config-mcast)# rate-per-route
```

Related Commands

Command	Description
#unique_151	

route-policy

To apply route policy to a neighbor, either to inbound routes or outbound routes, use the **route-policy** command in the BGP neighbor address-family configuration mode. To disable this feature, use the **no** form of this command.

route-policy *policy_name* [**in** | **out**]

Syntax Description

policy-name	Specifies the name of the route policy.
in	Applies route policy to inbound routes.
out	Applies route policy to outbound routes.

Command Default

No default behavior or values

Command Modes

BGP Neighbor Address-family Configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
multicast	read, write

```
RP/0/(config-bgp-nbr)# address-family vpnv4 unicast
RP/0/(config-bgp-nbr-af)# route-policy pass-all in
RP/0/(config-bgp-nbr-af)# route-policy pass-all out
```

shared-tree-prune delay

To set or change the prune installation time, use the **shared-tree-prune-delay**command in the appropriate mode. To disable the set time, use the **no** form of the command.

shared-tree-prune-delay *time*
noshared-tree-prune-delay *time*

Syntax Description

time	Delay in seconds. Range is 0 to 1800.

Command Default

60 seconds (for upstream prune)

Command Modes

C-multicast-routing configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command is used to change the prune installation time(C-S, C-G, RPT). This is required on PEs connected to the C-RP (under certain conditions), when a Type-5 route is received. This is applicable only to BGP C-multicast Routing.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **shared-tree-prune-delay** command:

```
RP/0/ (config-pim-v1-ipv4-mdt-cmcast) # shared-tree-prune-delay 100
```

show mfib connections

To display the status of Multicast Forwarding Information Base (MFIB) connections to servers, use the **show mfib connections** command in the appropriate mode.

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
location *node-id*	(Optional) Specifies MFIB connections associated with an interface of the designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show mfib connections** command to display a list of servers connected to the MFIB and the status of the connections.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib connections** command:

```
RP/0/# show mfib connections

Netio            : connected
IM               : connected
Pakman           : connected
MRIB             : connected
IFH              : connected
SysDB-Global     : connected
SysDB-Local      : connected
SysDB-NSF        : connected
SYSDB-EDM        : connected
SYSDB-Action     : connected
AIB              : connected
MLIB             : connected
IDB              : connected
IIR              : connected
```

```
IPARM              : connected
GSP                : connected
```

Related Commands

Command	Description
show mfib interface, on page 252	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
#unique_151	

show mfib counter

To display Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped, use the **show mfib counter** command in mode.

show mfib [**vrf** *vrf-name*] **ipv4 counter** [**location** *node-id*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
location *node-id*	(Optional) Specifies MFIB counter statistics associated with an interface of the designated node.

Command Default

IPv4 addressing is the default.

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show mfib counter** command displays packet drop statistics for packets that cannot be accounted for under route counters.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib counter** command:

```
RP/0/# show mfib counter location 0/1/CPU0

MFIB global counters are :
* Packets [no input idb]                   : 0
* Packets [failed route lookup]            : 0
* Packets [Failed idb lookup]              : 0
* Packets [Mcast disabled on input I/F]    : 0
* Packets [encap drops due to ratelimit]   : 0
* Packets [MC disabled on input I/F (iarm nfn)]      : 0
```

This table describes the significant fields shown in the display.

Table 34: show mfib counter Field Descriptions

Field	Description
Packets [no input idb]	Packets dropped because no input interface information was found in the packet.
Packets [failed route lookup]	Packets dropped because of failure to match any multicast route.

Field	Description
Packets [Failed idb lookup]	Packets dropped because the descriptor block was not found for an interface (incoming or outgoing).
Packets [Mcast disabled on input I/F]	Packets dropped because arriving on an interface that was not enabled for the multicast routing feature.
Packets [encap drops due to ratelimit]	Packets dropped because of rate limit.

Related Commands

Command	Description
show mfib interface, on page 252	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mfib route, on page 260	Displays route entries in the Multicast Forwarding Information Base (MFIB).

show mfib encap-info

To display the status of encapsulation information for Multicast Forwarding Information Base (MFIB), use the **show mfib encap-info** command in the appropriate mode.

show mfib [**vrf** *vrf-name*] [**ipv4** | **ipv6**] **encap-info** [**location** *node-id*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
location *node-id*	(Optional) Specifies MFIB connections associated with an interface of the designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib encap-info** command:

```
RP/0/# show mfib vrf vrf_a encap-info


                  ----------------------------
Encaps String                       Dependent  Encaps      MDT Name/
                                    Routes #   Table ID    Handle

(192.168.5.203, 255.1.1.1)            5          0xe0000000  mdtA1 (0x100a480)
```

Related Commands

Command	Description
show mfib interface, on page 252	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
#unique_151	

show mfib interface

To display interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process, use the **show mfib interface** command in EXEC mode.

show mfib [**vrf** *vrf-name*] **ipv4 interface** [*type interface-path-id*] [**detail** | **route**] [**location** *node-id*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
detail	(Optional) Specifies detailed information for packet statistics on interfaces.
route	(Optional) Specifies a list of routes associated with the interface. This option is available if an interface *type* and *instance* are specified.
location *node-id*	(Optional) Specifies packet statistics associated with an interface of the designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show mfib interface** command displays counters for the number of packets and bytes that are handled by software switching.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib interface** command for the multicast route on node 0/2/CPU0 that is associated with the Gigabit Ethernet interface 0/2/0/2:

```
Router# show mfib interface HundredGigE 0/0/0/24 location 0/2/CPU0

Interface : HundredGigE0/0/0/24 (Enabled)
Mcast pkts in : 5839, Mcast pkts out : 0 TTL Threshold : 0 Ref Count : 18
```

The following is sample output from the **show mfib interface** command with the **detail** and **location** keywords specified:

```
Router# show mfib interface detail location 0/2/CPU0

Interface : FINT0/2/CPU0 [0x3000000] (Disabled) PHYSICAL Create Unknown Mcast pkts in: 0,
Mcast pkts out: 0 TTL Threshold : 0, VRF ID: 0x60000000, Multicast Adjacency Ref Count: 2,
 Route Count: 0, Handle: 0x3000000 Primary address : 0.0.0.0/32 Secondary address : 0.0.0.0/32


Interface : HundredGigE0/0/0/24 [0x3000900] (Enabled) PHYSICAL Create Rcvd Mcast pkts in:
5844, Mcast pkts out: 0 TTL Threshold : 0, VRF ID: 0x60000000, Multicast Adjacency Ref
Count: 18, Route Count: 15, Handle: 0x3000900 Primary address : 112.112.112.203/24 Secondary
 address : 0.0.0.0/32
```

This table describes the significant fields shown in the display.

Table 35: show mfib interface Field Descriptions

Field	Description
Interface	Interface name. Enabled if the interface is configured for multicast routing. The word “PHYSICAL” is displayed if the interface is a nonvirtual interface.
Mcast pkts in	Number of incoming multicast packets entering the interface during software switching.
Mcast pkts out	Number of outgoing multicast packets exiting the interface during software switching.
TTL Threshold	Number of multicast packets that reach the configured multicast time-to-live threshold.
VRF ID	VPN Routing and Forwarding instance ID.
Ref Count	Number of references to this interface structure in the MFIB process.
Primary address	Primary IP address of the interface.
Secondary address	Secondary IP address of the interface.

show mfib nsf

To display the state of a nonstop forwarding (NSF) operation for the Multicast Forwarding Information Base (MFIB) line cards, use the **show mfib nsf** command in EXEC mode.

show mfib [**ipv4**] **nsf** [**location** *node-id*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
location *node-id*	(Optional) Specifies the MFIB NSF designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show mfib nsf** command displays the current multicast NSF state for the MFIB process contained on all line cards and route processors (RPs) in the router.

For multicast NSF, the state may be one of the following:

- **Normal—**Normal operation: The MFIBs in the card contain only up-to-date MFIB entries.
- **Boot Card Booting—**Card is initializing and has not yet determined its NSF state.
- **Not Forwarding—**Multicast Forwarding Disabled: Multicast routing failed to recover from a failure-induced NSF state prior to the MFIB NSF timeout.
- **Non-stop Forwarding Activated—**Multicast NSF active: The router is operating in NSF mode while attempting to recover from a control-plane failure. In this mode, data is forwarded based on MFIB entries that are either updated by the recovered Multicast Routing Information Base (MRIB), or MFIB entries that were marked stale when NSF mode began. The times remaining until multicast NSF and multicast-unicast NSF expiration are displayed.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib nsf** command:

```
RP/0/# show mfib nsf

IP MFWD Non-Stop Forwarding Status:
  NSF Lifetime: 00:15:00

On node 0/1/CPU0 :
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:54
```

```
On node 0/3/CPU0 :
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:54

On node 0/4/CPU0 :
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:53

On node 0/6/CPU0 :
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:53
```

This table describes the significant fields shown in the display.

Table 36: show mfib nsf Field Descriptions

Field	Description
IP MFWD Non-Stop Forwarding Status	MFIB NSF status of each node in the system: booting, normal, not forwarding, or activated.
NSF Time Remaining	If MSB NSF is activated, the time remaining until NSF fails and all routes are deleted displays. Before timeout, MRIB signals that NSF (in the control plane) is finished and new, updated routes are populated in the MFIB (which makes the transition to Normal status).

Related Commands

Command	Description
nsf lifetime (IGMP)	Configures the maximum time for the NSF timeout value under IGMP.
nsf (multicast) , on page 241	Configures the NSF capability for the multicast routing system.
nsf lifetime (PIM)	Configures the NSF timeout value for the PIM process.
show igmp nsf	Displays the state of NSF operation in IGMP.
show mrib nsf, on page 270	Displays the state of NSF operation in the MRIB.
show pim nsf	Displays the state of NSF operation for PIM.

show mfib platform route

To display route entries in the Multicast Forwarding Information Base (MFIB) specific to Cisco 8000 series routers, use the **show mfib platform route** command in EXEC mode.

show mfib [**vrf** *vrf-name*] **ipv4 platform route** [**statistics** | ***** *source-IP-address* | *group-IP-address* / **prefix-length** | **detail** | **summary** | **location** *node-id*]

Syntax Description

*****	(Optional) Display shared tree entries.
source-IP-address	(Optional) IP address or hostname of the multicast route source. Format is: *A.B.C.D*
group-IP-address	(Optional) IP address or hostname of the multicast group. Format is: *A.B.C.D*
/prefix-length	(Optional) Group IP prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). Format is: *A.B.C.D/length*
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
detail	(Optional) Specifies detailed route information.
location *node-id*	(Optional) Specifies an MFIB-designated node.
statistics	(Optional) Display both software and hardware forwarding statistics.
summary	(Optional) Displays a brief list of the routing database.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

All entries in the MFIB table are derived from the Multicast Routing Information Base (MRIB). The flags have the same connotation as in the MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets. In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry.

The **show mfib counter** command displays global counters independent of the routes.

This command displays counters for the number of packets and bytes that are handled by hardware switching.

Starting with Cisco IOS XR Software Release 25.1.1, the **show mfib route rate** command is supported on Bridge Group Virtual Interfaces (BVIs).

Platform commands for route rate calculate the instantaneous rate in every 30 seconds. Use the **show mfib route rate** and **show mrib route rate** commands for route rate calculations.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib platform route** command with the **location** keyword specified (the output fields are described in the header). The hardware and software specific information for the given multicast route is displayed in the output:

```
Router# show mfib platform route 232.100.1.1 detail loc 0/0/CPU0

------------------------------------------------------------------------------
Legend:
Route Information
    MC GID:    Multicast Index     NPI:     NP Independent

Outgoing Interface Information
    UL_Intf: Underlying Interface  UL_IFH:  Underlying Interface Handle
    L:       Local Interface       B:       Bundle Interface
    O:       In NPI Layer          OT:      OLE TYPE
    MRID:    Multicast Group Index
    SE:      Last sync error reported in OFA
    AE:      Last async error reported in OFA
------------------------------------------------------------------------------


VRF_ID: 0x0          Source: 1.1.1.1         Group: 232.100.1.1     Mask: 64

    SW Route Information
    ----------------------------
    RPF Intf: FH0/0/0/7/0                  RPF Intf_Handle:0x3e8
    Global MC GID:[Current:136  Old:0] Scale mode: Not-Set
    NPU MASK[Current:0x0  Old:0x0]         Total OLE_CNT:1
    Route Created in OFA: T                MC GID Created in OFA: T
    IC_Lo: F,  Signal: F                   NS_A_intf: F,  Encaps_Punt: F,
    Decaps_Punt: F                         RPF_fail: T
    RPFID: 1                               PD RPFID: 0     (Annot RPFID 23552)
    Encap ID: 0                            Encap MC GID:[Current:0  Old:0],
    Core Type: DECAP                       Overlay VRF ID:0
    Recycle NP: 0
    Protection MoFRR: Not-Set

    HW Route NPI Information
    ----------------------------
    RPF Interface Information
    RPF Intf:None                          RPF Intf_Handle:0x0
    L3If RefKey:0x0

    DPA Route Context Information
    MC GID:136              NPU BITMAP:0x0              VRF ID:0x0
    Punt Action:0x4         OFA_sync_route_rc:0x0       OFA_sync_mc_gid_rc:0x0
    OFA_async_route_rc:0x0  OFA_async_mc_gid_rc:0x0
    DPA_adapt_rc:0x0        DPA_map_rc:0x0              DPA_exec_rc:0x0
```

```
   DPA_post_rc:0x0
   Statistics [Enabled: Y]

VRF_ID: 0x0          Source: 2.2.2.2         Group: 232.100.1.1     Mask: 64

   SW Route Information
   ----------------------------
   RPF Intf: Lo0                          RPF Intf_Handle:0xf00001c
   Global MC GID:[Current:134  Old:0] Scale mode: Not-Set
   NPU MASK[Current:0x0  Old:0x0]         Total OLE_CNT:2
   Route Created in OFA: T                MC GID Created in OFA: T
   IC_Lo: F,  Signal: F                   NS_A_intf: F,  Encaps_Punt: F,
   Decaps_Punt: F                         RPF_fail: T
   RPFID: 1                               PD RPFID: 0     (Annot RPFID 23552)
   Encap ID: 0                            Encap MC GID:[Current:0  Old:0],
   Core Type: ENCAP                       Overlay VRF ID:0
   Recycle NP: 0
   Protection MoFRR: Not-Set

   HW Route NPI Information
   ----------------------------
   RPF Interface Information
   RPF Intf:None                          RPF Intf_Handle:0x0
   L3If RefKey:0x0

   DPA Route Context Information
   MC GID:134               NPU BITMAP:0x0               VRF ID:0x0
   Punt Action:0x4          OFA_sync_route_rc:0x0        OFA_sync_mc_gid_rc:0x0
   OFA_async_route_rc:0x0   OFA_async_mc_gid_rc:0x0
   DPA_adapt_rc:0x0         DPA_map_rc:0x0               DPA_exec_rc:0x0
   DPA_post_rc:0x0
   Statistics [Enabled: Y]

VRF_ID: 0x0          Source: 3.3.3.3         Group: 232.100.1.1     Mask: 64

   SW Route Information
   ----------------------------
   RPF Intf: FH0/0/0/3/0                  RPF Intf_Handle:0x3a8
   Global MC GID:[Current:135  Old:0] Scale mode: Not-Set
   NPU MASK[Current:0x0  Old:0x0]         Total OLE_CNT:1
   Route Created in OFA: T                MC GID Created in OFA: T
   IC_Lo: F,  Signal: F                   NS_A_intf: F,  Encaps_Punt: F,
   Decaps_Punt: F                         RPF_fail: T
   RPFID: 1                               PD RPFID: 0     (Annot RPFID 23552)
   Encap ID: 0                            Encap MC GID:[Current:0  Old:0],
   Core Type: DECAP                       Overlay VRF ID:0
   Recycle NP: 0
   Protection MoFRR: Not-Set

   HW Route NPI Information
   ----------------------------
   RPF Interface Information
   RPF Intf:None                          RPF Intf_Handle:0x0
   L3If RefKey:0x0

   DPA Route Context Information
   MC GID:135               NPU BITMAP:0x0               VRF ID:0x0
   Punt Action:0x4          OFA_sync_route_rc:0x0        OFA_sync_mc_gid_rc:0x0
   OFA_async_route_rc:0x0   OFA_async_mc_gid_rc:0x0
   DPA_adapt_rc:0x0         DPA_map_rc:0x0               DPA_exec_rc:0x0
   DPA_post_rc:0x0
```

```
Statistics [Enabled: Y]
```

Related Commands

Command	Description
show mfib route	Displays route entries in the Multicast Forwarding Information Base (MFIB).
show mfib counter, on page 249	Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.
show mfib interface, on page 252	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mrib route, on page 276	Displays all entries in the Multicast Routing Information Base (MRIB).

show mfib route

To display route entries in the Multicast Forwarding Information Base (MFIB), use the **show mfib route** command in EXEC mode.

show mfib [**vrf** *vrf-name*] **ipv4 route** **statistics** [**rate** | ***** *source-IP-address* | *group-IP-address* / **prefix-length** | **detail** | **summary** | **location** *node-id*]

Syntax Description

*****	(Optional) Display shared tree entries.
source-IP-address	(Optional) IP address or hostname of the multicast route source. Format is: *A.B.C.D*
group-IP-address	(Optional) IP address or hostname of the multicast group. Format is: *A.B.C.D*
/prefix-length	(Optional) Group IP prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). Format is: *A.B.C.D/length*
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
detail	(Optional) Specifies detailed route information.
location *node-id*	(Optional) Specifies an MFIB-designated node.
rate	(Optional) Displays individual (S, G) rates.
sources-only	(Optional) Restricts display of any shared-tree entries.
statistics	(Optional) Display both software and hardware forwarding statistics.
summary	(Optional) Displays a brief list of the routing database.
tech-support	(Optional) Displays technical support information.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

All entries in the MFIB table are derived from the Multicast Routing Information Base (MRIB). The flags have the same connotation as in the MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets. In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry.

The **show mfib counter** command displays global counters independent of the routes.

This command displays counters for the number of packets and bytes that are handled by software switching.
.

The command displays the cumulative rates per route for all line cards in the Multicast Forwarding Information Base (MFIB) table when the **rate** keyword is used with the source and group IP addresses.

Note To view accurate route statistics, run the **show mfib route statistics** command on the line card where the route traffic enters the router. This requirement does not apply to fixed or centralized systems.

On Cisco Silicon One Q100- and Q200-based systems, if the ingress interface is a virtual interface, such as a Bundle-Ether interface, MFIB reports the route statistics on the Multicast Line Card (MLC).

To identify the MLC, use the **show mrib platform stats-ole slot all summary** command. In the output, the line card with the **Is MLC : T** field is the MLC.

Task ID

Task ID	Operations
multicast	read

```
RP/0/RP0/CPU0:r5# show mrib platform stats-ole slot all summary
Thu Apr 2 11:34:32.789 EDT

LC Slot : 0 Total NP : 1 OOR State : GREEN Is MLC : T
============================================================
NP fapid OOR Max Used Free Usage
============================================================
0 0x0 GREEN 64000 0 64000 0.000000%
============================================================
```

Related Commands

Command	Description
show mfib counter, on page 249	Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.
show mfib interface, on page 252	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mrib route, on page 276	Displays all entries in the Multicast Routing Information Base (MRIB).

show mfib table-info

To display Multicast Forwarding Information Base (MFIB) table information, use the **show mfib table-info** command in EXEC mode.

show mfib [**ipv4** | **ipv6**] **table-info** {*table-idvrf-name*} [**local** | **remote**] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
table-id	Specifies the table identifier. Range is 0 to 4294967295.
vrf-name	Specifies the VRF name.
local	Specifies local tables only.
remote	Specifies remote tables only.
location *node-id*	(Optional) Specifies MFIB connections associated with an interface of the designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib table-info** command:

```
RP/0/# show mfib table-info table-id location 0/0/CPU0

Table Name           : default
VRid/TID/VID         : 0x0 / 0xe0000000 / 0x60000000
Table type           : TBL_TYPE_TID
Active/Linked        : Y / Y
Prev Table ID        : 0x0
Location             : Local
Local ifcount        : 16
Default MDT Encap    : (*, */32)
MDT Master LC        : N
Loopback (Encap Src) : 0x0 (Ha0x0)
```

```
Local EG intf cnt    : 6
Data MDT             : Acl - (-), All vrf routes N, 0 Kbps


RP/0/#show mfib table-info vrf 101

Table Name           : vrf15
VRid/TID/VID         : 0x0 / 0xe000000f / 0x6000000f
Table type           : TBL_TYPE_NAME_VID
Active/Linked        : Y / Y
Prev Table ID        : 0x0
Location             : Local
Local ifcount        : 2
Child routes         : (5.5.5.5, 225.101.1.15/32)

Default MDT Handle   : 0x0 (Ha0x0)


MDT Master LC        : Y
Loopback (Encap Src) : 0x9000180 (Loopback0)
Local EG intf cnt    : 508
Data MDT             : Acl - (-), All vrf routes N, 0 Kbps
```

This table describes the significant fields shown in the display.

Table 37: show mfib table-info Field Descriptions

Field	Description
Table Name	Name of the MFIB table.
VRid/TID/VID	Table identifiers.
Table type	Type of MFIB table.
Active/Linked	Table is active and linked.
Location	Location of the MFIB table.
Local ifcount	Local interface count.
Child routes	Child routes shows the number of extranet routes in receiver VRFs that reference this source VRF.
Default MDT Encap	Default MDT encapsulation.
Default MDT Handle	Default MDT interface handle for this VRF.
MDT Master LC	Field contains "Y" if this line card is a master line card for this VRF.
Loopback (Encap Src)	Loopback (encapsulation source).
Local EG intf cnt	Shows the number of local egress interfaces for this VRF and location.
Data MDT	Routes for which multicast data for a multicast distribution tree (MDT) was triggered.

show mrib client

To display the state of the Multicast Routing Information Base (MRIB) client connections, use the **show mrib client** command in the appropriate mode.

show mrib [**vrf** *vrf-name*] **ipv4 client** [**filter**] [*client-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
filter	(Optional) Displays route and interface level flag changes that various MRIB clients have registered and shows what flags are owned by the MRIB clients.
client-name	(Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as Protocol Independent Multicast (PIM) or Internet Group Management Protocol (IGMP).

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib client** command using the **filter** option:

```
RP/0/# show mrib client filter

IP MRIB client-connections
igmp:417957 (connection id 0)
 ownership filter:
  interface attributes: II ID LI LD
  groups:
   include 0.0.0.0/0
  interfaces:
   include All
pim:417959 (connection id 1)
 interest filter:
  entry attributes: E
  interface attributes: SP II ID LI LD
  groups:
   include 0.0.0.0/0
```

```
  interfaces:
   include All
 ownership filter:
  entry attributes: L S C IA IF D
  interface attributes: F A IC NS DP DI EI
  groups:
   include 0.0.0.0/0
  interfaces:
   include All
bcdl_agent:1 (connection id 2)
 interest filter:
  entry attributes: S C IA IF D
  interface attributes: F A IC NS DP SP EI
  groups:
   include 0.0.0.0/0
  interfaces:
   include All
 ownership filter:
  groups:
   include 0.0.0.0/0
  interfaces:
   include All
```

This table describes the significant fields shown in the display.

Table 38: show mrib client Field Descriptions

Field	Description
igmp	Name of the client.
417957	Personal identifier (PID) or a unique ID assigned by MRIB.
(connection id 0)	Unique client connection identifier.
ownership filter:	Specifies all the route entry and interface-level flags that are owned by the client. As the owner of the flag, only the client can add or remove the flag. For example, only the Internet Group Management Protocol (IGMP) client can add the II flag on an interface. MRIB does not allow a non-owner to register or modify the same flag.
groups: include 0.0.0.0/0interfaces: include All	Groups and interfaces registered by the clients consisting of two lists. One is an include list (items for which the client requests to be notified.) The use of "All" implies all interfaces and 0.0.0.0/0 to indicate all groups. Not shown in this example is the exclude list. This list contains items for which the client requests not to be notified when modifications occur.
interface attributes: II ID LI LD	Interface-level flags set on the interface belong to a route.
interest filter:	Specifies all the flags, groups, and interfaces from which the client requests information. When a flag of interest for a client is modified, the client is notified.

Field	Description
entry attributes: S C IA IF D	Entry-level flags that are set on the route.

Related Commands

Command	Description
show mfib nsf, on page 254	Displays the state of a nonstop forwarding (NSF) operation for the Multicast Forwarding Information Base (MFIB) line cards.
#unique_151	
show mrib nsf, on page 270	Displays the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB).

show mrib mpls forwarding

To display the Multicast Routing Information Base (MRIB) MPLS forwarding table information of all tunnels, use the **show mrib mpls forwarding** command in

EXEC mode

.

show mrib mpls forwarding [**detail** | **labels** | **s2l** | **source** | **summary** | **tunnels**]

Syntax Description

detail	Provides the detail information of each tunnel.
labels	Filters based on label.
s2l	Filters based on s2l.
source	Filters based on source PE address.
summary	Displays the summary output of entries.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is a sample output from the **show mrib mpls forwarding** command:

```
RP/0/# show mrib mpls forwarding

LSP information (RSVP-TE) :
  Name: tunnel-mte26 Role: Head State: binding
    TUNNEL-ID: 26  P2MP-ID: 26  LSP-ID: 10012
    Source Address: 192.1.1.1  Extended-ID: 192.1.1.1(0xc0010101)

      Incoming Label       : (16008)
      Transported Protocol : IPv4
      Explicit Null        : IPv6 Explicit Null
      IP lookup            : enabled

      Outsegment Info #1 [Head/Push]:
        Outgoing Label: 16008  Outgoing IF: GigabitEthernet0/0/0/5(P) Outgoing Node ID: 0x1
```

```
  Nexthop: 192.14.1.44


LSP information (RSVP-TE) :
  Name: tunnel-mte27 Role: Head State: binding
    TUNNEL-ID: 27  P2MP-ID: 27  LSP-ID: 10012
    Source Address: 192.1.1.1  Extended-ID: 192.1.1.1(0xc0010101)

      Incoming Label       : (16007)
      Transported Protocol : IPv4
      Explicit Null        : IPv6 Explicit Null
      IP lookup            : enabled
      Platform information : FGID: 51075, 51076 frr_slotmask: 0x1

      Outsegment Info #1 [Head/Push]:
        Outgoing Label: 16007  Outgoing IF: GigabitEthernet0/0/0/5(P) Outgoing Node ID: 0x1
  Nexthop: 192.14.1.44
```

The following is a sample output from the **show mrib mpls forwarding** command with the detail keyword:

```
RP/0/# show mrib mpls forwarding tunnel 27 detail

LSP information (RSVP-TE) :
  Name: ------ Role: Bud
    TUNNEL-ID: 27  P2MP-ID: 27  LSP-ID: 10002
    Source Address: 192.1.1.1  Extended-ID: 192.1.1.1(0xc0010101)

      Incoming Label       : 16001
      Transported Protocol : IPv4
      Explicit Null        : IPv6 Explicit Null
      IP lookup            : enabled
      Platform information : FGID: 44045, 44046 frr_slotmask: 0x24

      Outsegment Info #1 [Tail/Pop]:
        No info.
      Outsegment Info #2 [Mid/Swap]:
        Outgoing Label: 16001  Outgoing IF: GigabitEthernet0/5/0/6(P) Outgoing Node ID:
0x51  Nexthop: 192.168.12.2
      Outsegment Info #3 [Mid/Swap]:
        Outgoing Label: 16001  Outgoing IF: GigabitEthernet0/2/0/4(P) Outgoing Node ID:
0x21  Nexthop: 192.168.13.2

RP/0/# show mrib mpls forwarding tunnel 26 detail

LSP information (RSVP-TE) :
  Name: ------ Role: Tail
    TUNNEL-ID: 26  P2MP-ID: 26  LSP-ID: 10012
    Source Address: 192.1.1.1  Extended-ID: 192.1.1.1(0xc0010101)

      Incoming Label       : 16008
      Transported Protocol : IPv4
      Explicit Null        : IPv6 Explicit Null
      IP lookup            : enabled
      Platform information : FGID: 51082, 51083 frr_slotmask: 0x0
Outsegment Info #1 [Tail/Pop]:
        No info.
```

show mrib mpls route

To display the Multicast Routing Information Base (MRIB) multicast groups to tunnels mappings, use the **show mrib mpls route** command in EXEC mode.

show mrib mpls route [**interface** | **summary**]

Syntax Description

interface	(Optional) Specify the type of interface.
summary	(Optional) Displays the summary information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

This is a sample output from the **show mrib mpls route** command:

```
RP/0/# show mrib mpls route

Tunnel Interface: tunnel-mte28
    (192.19.1.9, 239.232.2.1) (192.19.1.9, 239.232.2.2) (192.19.1.9, 239.232.2.3)
Tunnel Interface: tunnel-mte27
    (192.19.1.9, 239.232.1.1) (192.19.1.9, 239.232.1.2) (192.19.1.9, 239.232.1.3)
Tunnel Interface: tunnel-mte26
    (192.19.1.9, 239.232.0.1) (192.19.1.9, 239.232.0.2) (192.19.1.9, 239.232.0.3)
```

show mrib nsf

To display the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB), use the **show mrib nsf** command in the appropriate mode.

show mrib ipv4 nsf

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show mrib nsf** command displays the current multicast NSF state for the MRIB. The state may be normal or activated for NSF. The activated state indicates that recovery is in progress due to a failure in MRIB or Protocol Independent Multicast (PIM). The total NSF timeout and time remaining are displayed until NSF expiration.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib nsf** command:

```
RP/0/# show mrib nsf

IP MRIB Non-Stop Forwarding Status:
Multicast routing state: Non-Stop Forwarding Activated
NSF Lifetime: 00:03:00
NSF Time Remaining: 00:01:40
```

This table describes the significant fields shown in the display.

Table 39: show mrib nsf Field Descriptions

Field	Description
Multicast routing state	Multicast NSF status of the MRIB (Normal or NSF Activated).
NSF Lifetime	Timeout for MRIB NSF, computed as the maximum of the PIM and Internet Group Management Protocol (IGMP) NSF lifetimes, plus 60 seconds.

Field	Description
NSF Time Remaining	If MRIB NSF state is activated, the time remaining until MRIB reverts to Normal mode displays. Before this timeout, MRIB receives notifications from IGMP and PIM, triggering a successful end of NSF and cause the transition to normal state. If notifications are not received, the timer triggers a transition back to normal mode, causing new routes to download to MFIB and old routes to be deleted.

Related Commands

Command	Description
nsf (multicast) , on page 241	Configures the NSF capability for the multicast routing system.
nsf lifetime (IGMP)	Configures the maximum time for the NSF timeout value under IGMP.
nsf lifetime (PIM)	Configures the NSF timeout value for the PIM process.
show igmp nsf	Displays the state of NSF operation in IGMP.
show mfib nsf	Displays the state of NSF operation in the MFIB line cards.
show pim nsf	Displays the state of NSF operation for PIM.

show mrib nsr end

To display nonstop routing (NSR) operation in the Multicast Routing Information Base (MRIB), use the **show mrib nsr end** command in the appropriate mode.

show mrib ipv4| ipv6 nsr end

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command after an NSR event (for example, RPFO or a process restart) to determine when each of the MRIB or MRIB6's NSR clients finished re-downloading the information to the MRIB and if any previously downloaded information was purged in the process.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib nsr end** command:

```
RP/0/# show mrib nsr end
Time                Client       Idx    Change
Oct 17 18:43:36     Membership   1      N
Oct 17 18:43:40     Routing      2      Y
```

This table describes the significant fields shown in the display.

Table 40: show mrib nsr end Field Descriptions

Field	Description
Time	The time at which the client finished downloading information back to MRIB or MRIB6 after the NSR event.
Client	Client type (Membership - IGMP/MLD, Routing - PIM/PIM6)
Change	Was there an route or interface attribute purge Y - yes, N - no

Related Commands

Command	Description
show msdp nsr	Displays the state of NSR operation for MSDP.
show igmp nsr	Displays the state of NSR operation for IGMP.
show pim nsr	Displays the state of NSR operation for PIM.

show mrib route-collapse

To display the contents of the Multicast Routing Information Base (MRIB) route-collapse database, use the **show mrib route-collapse** command in the appropriate mode.

show mrib [**vrf** *vrf-name*] **ipv4 route-collapse** [*core-tree*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
core-tree	(Optional) IPv4 Multicast Distribution Tree (MDT) group address.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib route-collapse** command:

```
RP/0/# show mrib route-collapse

226.1.1.1  TID: 0xe0000038   TLC TID: 0xe0000038
  Customer route database count: 5
    (192.168.5.204,224.0.1.40/32)
    (*,226.226.226.226/32)
    (*,228.228.228.228/32)
    (192.168.113.17,228.228.228.228/32)
    (*,229.229.229.229/32)
  Core route database count: 4
    (*,226.1.1.1/32)
    (192.168.5.201,226.1.1.1/32)
    (192.168.5.202,226.1.1.1/32)
    (192.168.5.204,226.1.1.1/32)
  Core egress node database count: 1
    nodeid        slot            refcount
    0x20          0/2/CPU0        1

192.168.27.1  TID: 0xe0000039   TLC TID: 0xe0000039
  Customer route database count: 1
    (192.168.113.33,227.227.227.227/32)
  Core route database count: 3
    (*,227.27.27.1/32)
```

```
    (192.168.5.201,227.27.27.1/32)
    (192.168.5.202,227.27.27.1/32)
  Core egress node database count: 1
    nodeid        slot            refcount
    0x20          0/2/CPU0        1

192.168.28.1  TID: 0xe000003a   TLC TID: 0xe000003a
  Customer route database count: 2
    (192.168.5.204,224.0.1.40/32)
    (192.168.113.49,229.229.229.229/32)
  Core route database count: 3
    (192.168.5.201,228.28.28.1/32)
    (192.168.5.202,228.28.28.1/32)
    (192.168.5.204,228.28.28.1/32)
  Core egress node database count: 1
    nodeid        slot            refcount
    0x20          0/2/CPU0        1
```

Related Commands

Command	Description
show mrib route, on page 276	Displays all entries in the Multicast Routing Information Base (MRIB).

show mrib route

To display all entries in the Multicast Routing Information Base (MRIB), use the **show mrib route** command in mode.

show mrib [**vrf** *vrf-name*] [**ipv4** | **ipv6**] [**old-output**] **route** [**summary** | **outgoing-interface** | [**rate** | ***** *source-address*] [*group-address* [/ *prefix-length*]]] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
*****	(Optional) Displays shared tree entries.
source-address	(Optional) Source IP address or hostname of the MRIB route. Format is: *A.B.C.D* or *X:X::X.*
group-address	(Optional) Group IP address or hostname of the MRIB route. Format is: *A.B.C.D* or *X:X::X.*
/prefix-length	(Optional) Prefix length of the MRIB group address. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Format is: *A.B.C.D* or *X:X::X.*
rate	(Optional) Displays individual (S, G) rates.
outgoing-interface	(Optional) Displays the outgoing-interface information.
summary	(Optional) Displays a summary of the routing database.
detail	(Optional) Displays the routing database with the platform data.

Command Default

IPv4 addressing is the default.

Command Modes

Command History

Release 7.0.12 This command was introduced.

Usage Guidelines

Each line card has an individual Multicast Forwarding Information Base (MFIB) table. The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets. In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry.

The show mfib counter, on page 249 command displays global counters independent of the routes.

Starting Cisco IOS XR Software Release 24.4.1, the route statistics counter is programmed on the ingress line card for the Cisco Silicon One P100 ASIC-based Systems.

The `stats-ole` counter-based implementation is activated when at least one of the Cisco Silicon One Q100 or Q200 ASIC-based systems, along with the Cisco Silicon One P100 ASIC-based systems, is operational on a router.

When `stats-ole` counter-based implementation is active, the **show mrib route detail** command output shows the `stats-ole` location; otherwise, it shows `INVALID`.

Task ID

Task ID	Operations
multicast	read

This example shows the truncated output for **show mrib route detail** command on the Cisco Silicon One P100 ASIC-based Systems:

```
Router # show mrib vrf vpn101 route detail
IP Multicast Routing Information Base
Entry flags:
- L - Domain-Local Source
- E - External Source to the Domain
- C - Directly-Connected Check
.
.
.

Interface flags:
- F - Forward
- A - Accept
- IC - Internal Copy
.
.
.

(*,224.0.0.0/4) Ver: 0x6119 RPF nbr: 198.51.100.1 Flags: L C RPF P, MRID: 9, MCGID: 40,
FLAGS: 0x0, Stats(F)
  Up: 00:03:12
  Outgoing Interface List
    Decapstunnel0 Flags: NS DI, Up: 00:03:07
(*,224.0.0.0/24) Ver: 0xc1d8 Flags: D P, MRID: 7, MCGID: 38, FLAGS: 0x0, Stats(F)
  Up: 00:03:12
(*,224.0.1.39) Ver: 0x653 Flags: S P, MRID: 5, MCGID: 36, FLAGS: 0x0, Stats(F)
  Up: 00:03:12
(*,224.0.1.40) Ver: 0xde67 Flags: S P, MRID: 6, MCGID: 37, FLAGS: 0x0, Stats(F)
  Up: 00:03:12
  Outgoing Interface List
    HundredGigE0/0/0/14 Flags: II LI, Up: 00:03:12
(*,232.0.0.0/8) Ver: 0x665b Flags: D P, MRID: 8, MCGID: 39, FLAGS: 0x0, Stats(F)
  Up: 00:03:12
(198.51.100.2,232.0.0.1) Ver: 0x710e RPF nbr: 203.0.113.1 Flags: RPF RPFID, MRID: 10, MCGID:
 136, FLAGS: 0x1, Stats(T): INVALID
  Up: 00:03:05
  RPF-ID: 1, Encap-ID: 0
  Incoming Interface List
    Lmdtvpn101 Flags: A LMI, Up: 00:02:43
  Outgoing Interface List
    HundredGigE0/0/0/14 Flags: F NS LI, Up: 00:03:05
```

Related Commands

Command	Description
show mfib counter, on page 249	Displays MFIB counter statistics for packets that have dropped.
show mrib route-collapse, on page 274	Displays the contents of the MRIB route collapse database.
show mfib route, on page 260	Displays all entries in the MFIB table.

show mrib route outgoing-interface

To display the outgoing-interface information on the Multicast Routing Information Base (MRIB), use the **show mrib route outgoing-interface** command in the appropriate mode.

show mrib route outgoing-interface [***source-address**] [*group-address* [*/prefix-length*]]

Syntax Description

*	(Optional) Displays shared tree entries.
A.B.C.D	(Optional) Source IP address or hostname of the MRIB route. Format is: *A.B.C.D*
A.B.C.D	(Optional) Group IP address or hostname of the MRIB route and the prefix length.
/prefix-length	(Optional) Prefix length of the MRIB group address. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Format is: *A.B.C.D*

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib route outgoing-interface** command:

```
RP/0/# show mrib route outgoing-interface

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, MA - MDT Address, ME - MDT Encap,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, MF - MPLS Encap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State

(*,224.0.0.0/4), Up:6d10h, OIF count:0, flags: C
(*,224.0.0.0/24), Up:6d10h, OIF count:0, flags: D
(*,224.0.1.39), Up:6d10h, OIF count:3, flags: S
(10.1.1.1,224.0.1.39), Up:6d10h, OIF count:11, flags:
```

```
(10.2.2.2,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.3.3.3,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.4.4.4,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.5.5.5,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.6.6.6,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.7.7.7,224.0.1.39), Up:00:04:17, OIF count:11, flags:
(10.8.8.8,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.9.9.9,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.10.10.10,224.0.1.39), Up:6d10h, OIF count:11, flags:
(10.21.21.21,224.0.1.39), Up:6d06h, OIF count:11, flags:
(*,224.0.1.40), Up:6d10h, OIF count:2, flags: S
(10.1.1.1,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.2.2.2,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.6.6.6,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.13.4.3,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.14.4.4,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.14.8.4,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.21.21.21,224.0.1.40), Up:6d06h, OIF count:11, flags:
(10.23.4.3,224.0.1.40), Up:00:02:38, OIF count:11, flags:
(10.23.8.3,224.0.1.40), Up:00:02:38, OIF count:11, flags:
(10.34.4.3,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.34.8.3,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.35.4.3,224.0.1.40), Up:00:02:38, OIF count:11, flags:
(10.35.4.5,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.38.4.8,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.45.4.5,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.49.4.9,224.0.1.40), Up:6d10h, OIF count:11, flags:
(10.105.4.10,224.0.1.40), Up:6d10h, OIF count:11, flags:
(*,225.0.0.0/8), Up:6d06h, OIF count:0, flags: C
(*,226.0.0.0/8), Up:6d06h, OIF count:0, flags: C
(*,232.0.0.0/8), Up:6d10h, OIF count:0, flags: D
(10.6.6.6,232.1.1.1), Up:6d10h, OIF count:3, flags:
(10.7.7.7,232.1.1.1), Up:6d10h, OIF count:2, flags:
(10.8.8.8,232.1.1.1), Up:6d10h, OIF count:2, flags:
(10.9.9.9,232.1.1.1), Up:6d10h, OIF count:2, flags:
(10.10.10.10,232.1.1.1), Up:6d10h, OIF count:2, flags:
(10.21.21.21,232.1.1.1), Up:6d06h, OIF count:3, flags:
```

Related Commands

Command	Description
show mrib route, on page 276	Displays all entries in the Multicast Routing Information Base (MRIB).

show mrib table-info

To display Multicast Routing Information Base (MRIB) table information, use the **show mrib table-info** command in the appropriate mode.

show mrib [**vrf** *vrf-name*] **ipv4 table-info**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib table-info** command:

```
RP/0/# show mrib vrf vrf101 table-info

VRF: default [tid 0xe0000000]
Registered Client:
  igmp [ccbid: 0 cltid: 4485366]
  pim [ccbid: 1 cltid: 4485368]
  bcdl_agent [ccbid: 2 cltid: 1]
  msdp [ccbid: 3 cltid: 8827135]
```

Table 41: show mrib table-info Field Descriptions

Field	Description
VRF	Default VRF or a VRF configured for the purpose of an override in MVPN.
cltid	Client ID.
bcdl_agent	A process like igmp and pim, which is used to download routes to line card.
MDT handle	MDT interface handle for this VRF.
MDT group	Default MDT group associated with this VRF.

Field	Description
MDT source	Per-VRF MDT source information.

Related Commands

Command	Description
show mrib tlc, on page 283	Displays the contents of the Multicast Routing Information Base (MRIB) table-line card (TLC) database.

show mrib tlc

To display the contents of the Multicast Routing Information Base (MRIB) table-line card (TLC) database, use the **show mrib tlc** command in the appropriate mode .

show mrib [**vrf** *vrf-name*] **ipv4 tlc**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib tlc** command:

```
RP/0/# show mrib tlc

VRF: default [tid 0xe0000000]
Master LC slot: Not selected
Associated MDT group: 0
Forwarding LC node: 0
```

This table describes the significant fields shown in the display.

Table 42: show msdp peer Field Descriptions

Field	Description
Associated MDT group	IP address of the MSDP peer.
Master LC slot	Indicates whether the master LC slot has been selected.
Forwarding LC node	Autonomous system to which the peer belongs.
Associated MDT group	Indicates the number of associated MDT groups.

show mrib vrf vrf_name route

To display the detail routing DB with platform data information for multicast routing information base, use the **show mrib vrf** *vrf_name* **route** command in the EXEC mode.

show mrib vrf *vrf_name* **route** *ip_address* **detail**

Syntax Description

detail	Displays routing DB with platform data.
ip_address	Specifies the group IP address.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

To enable statistics for VRF routes, configure both **rate-per-route** and **accounting per-prefix** under multicast-routing address-family.

Task ID

Task ID	Operation
multicast	read

```
RP/0/# show mrib vrf vrf1 route  232.1.1.1 detail
(192.1.1.2,232.1.1.1) Ver: 0x32b9 RPF nbr: 192.1.1.2 Flags: EID,
 PD: Slotmask: 0x0
     MGID: 17754
  Up: 12:35:50, Route node: 0x504f8df8
  RPF-ID: 0, Encap-ID: 4, EPtr: 0x505463c4, Hd: 0x502df6f8, Cts: 1, 0, 0, 0
  Acc: 1 (MDT: 0), Fwd: 1 (0), SRD: (0,0), Encap-next: 0x0
  Incoming Interface List
    GigabitEthernet0/0/0/1.1 Flags: A, Up: 05:30:09, Ptrs: 0x502df438, 0x0
  Outgoing Interface List
    tunnel-mte1 Flags: F NS LI LVIF, Up: 12:35:50, Ptrs: 0x502df6f8, 0x0
       LI add redist count: 2
```

source-tree-prune-delay

To set the delay-time for the (S,G) prune of the ingress-PE (provider edge), use the **source-tree-prune-delay** command in the appropriate mode. To remove the set delay, use the **no**form of the command.

source-tree-prune-delay *time*
nosource-tree-prune-delay *time*

Syntax Description

time	Delay in seconds. Range is 0 to 300.

Command Default

60 seconds

Command Modes

C-multicast-routing configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command is used to delay (S,G) Prune on the Ingress-PE, when the last Type-7 route is withdrawn.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **source-tree-prune-delay** command:

```
RP/0/ (config-pim-v1-ipv4-mdt-cmcast) # source-tree-prune-delay 100
```

static-rpf

To configure a static Reverse Path Forwarding (RPF) rule for a specified prefix mask, use the **static-rpf** command in an appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

static-rpf *prefix-address prefix-mask type path-id next-hop-address*
no static-rpf

Syntax Description

prefix-address	IP address of a prefix for an address range.
prefix-mask	Prefix mask for an address range. Range is 0 to 32 for IPv4 .
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
next-hop-address	IP address for an RPF neighbor.

Command Default

A static RPF rule for a specified prefix mask is not configured.

Command Modes

Multicast routing address family ipv4 and ipv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **static-rpf** command is used to configure incompatible topologies for unicast and multicast traffic.

Use the **static-rpf** command to configure a static route to be used for RPF checking in Protocol Independent Multicast (PIM) instead of using the unicast routing table.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example configures the static RPF rule for IP address 10.0.0.1:

```
Router(config)# multicast-routing
```

```
Router(config-mcast)# vrf green
Router(config-mcast)# static-rpf 10.0.0.1 32 HundredGigE 10.1.1.1
```

Related Commands

Command	Description
show pim context	Displays reverse path forwarding (RPF) table information configured for a VRF context.

suppress-pim-data-signaling

To suppress PIM data signaling, use the **suppress-pim-data-signaling** command in the appropriate mode. To remove the suppressed condition, use the **no** form of the command.

suppress-pim-data-signaling
nosuppress-pim-data-signaling

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

PIM C-multicast routing configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command supports c-anycast RP and can be used only under the PIM c-multicast routing mode.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **suppress-pim-data-signaling**command:

```
RP/0/ (config-pim-v1-ipv4-mdt-cmcast) # suppress-pim-data-signaling
```

suppress-shared-tree-join

To suppress shared tree joins and support the SPT-only mode, use the **suppress-shared-tree-join** command in the appropriate mode.

To remove the suppress condition, use the **no**form of the command.

suppress-shared-tree-join
nosuppress-shared-tree-join

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

C-multicast-routing configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command enables the SPT-only (Shortest Path Tree) mode.

Task ID

Task ID	Operation
multicast	read, write

Example

This command shows how to use the **suppress-shared-tree-join** command:

```
RP/0/(config-pim-v1-ipv4-mdt-cmcast) # suppress-shared-tree-join
```

unicast-reachability

To disable VPN-IP attributes, use the **unicast-reachability** command in the appropriate mode. To restore the attributes, use the **no**form of the command.

unicast-reachability [**connector-disable** | **source-as-disable** | **vrf-route-import-disable**]
nounicast-reachability [**connector-disable** | **source-as-disable** | **vrf-route-import-disable**]

Syntax Description

connector-disable	Disables connector addition.
source-as-disable	Disables source AS extended community addition.
vrf-route-import-disable	Disables VRF route import extended community addition.

Command Default

None

Command Modes

C-multicast routing configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command controls addition of extended communities to unicast VPN-IP routes. These attributes have specific purposes in PIM and BGP C-multicast Routing.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **unicast-reachability** command:

```
RP/0/ (config-pim-v1-ipv4-mdt-cmcast) # unicast-reachability connector-disable
```

vrf (multicast)

To configure a virtual routing and forwarding (VRF) instance for a VPN table, use the **vrf** command in multicast routing configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the **no** form of this command.

vrf *vrf-name* **ipv4**
no vrf *vrf-name* **ipv4**

Syntax Description

vrf-name	Name of the VRF instance. The following names cannot be used: all, default, and global.
ipv4	(Optional) Configures IPv4 address prefixes.

Command Default

No default behavior or values.

Command Modes

Multicast routing configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure a VRF instance and enter VRF configuration mode:

```
RP/0/(config)# multicast-routing
RP/0/(config-mcast)# vrf vrf_1
RP/0/(config-mcast-vrf_1-ipv4)# mdt ?

data     Data MDT group configuration
default  MDT default group address
mtu      MDT mtu configuration
source   Interface used to set MDT source address
```

Related Commands

Command	Description
accounting per-prefix, on page 209	Enables per-prefix counters only in hardware.
interface (multicast), on page 230	Configures multicast interface properties.
log-traps, on page 232	Enables logging of trap events.

Command	Description
multipath, on page 239	Enables Protocol Independent Multicast (PIM) to divide the multicast load among several equal-cost paths.
rate-per-route, on page 244	Enables individual (source, group [S, G]) rate calculations.
ssm	Defines the Protocol Independent Multicast (PIM)-Source Specific Multicast (SSM) range of IP multicast addresses.
static-rpf, on page 286	Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.



Hardware Module Commands

This module lists the hardware module commands for the Multicast configuration on the Cisco 8000 Series Routers.

For detailed information about the hardware module configuration tasks and examples, refer to the *Multicast Configuration Guide for Cisco 8000 Series Routers*.

- Hardware Module Commands, on page 294

Hardware Module Commands

Multicast Routing Forwarding Commands

- hw-module multicast route-scale, on page 225
- hw-module route-stats



INDEX

A

accept-register command 95
access-group (IGMP/MLD) command 2
accounting per-prefix command 209
address-family (multicast) command 211
auto-rp candidate-rp command 96

B

bsr candidate-bsr command 98
bsr candidate-rp command 100

C

cache-sa holdtime command 54
cache-sa-state command 52
clear igmp counters command 3
clear igmp group command 5
clear igmp reset command 7
clear mfib counter command 214
clear mfib database command 215
clear msdp peer command 55
clear msdp sa-cache command 56
clear msdp stats command 57
clear pim counters command 102
clear pim topology command 105
connect-source command 58

D

default-peer command 60
description (peer) command 61
disable (multicast) command 218
dr-priority command 107

E

enable (multicast) command 220
explicit-tracking command 8

F

forwarding-latency command 222

G

global maximum bsr crp-cache threshold 109, 111
global maximum command 108

H

hello-interval (PIM) command 113

I

interface (multicast) command 230
interface (PIM) command 115
interface all enable command 228
interface-inheritance disable command 226

J

join-group command 10
join-prune-interval command 117

L

log-traps command 232

M

maximum disable command 233
maximum external-sa command 62
maximum groups command 12
maximum groups-per-interface command 15
maximum peer-external-sa command 64
maximum register-states command 119
maximum route-interfaces command 120
maximum routes command 121
mesh-group (peer) command 65
mofrr command 122
multicast-routing command 238
multipath command 239

N

neighbor-check-on-recv enable command 124
neighbor-check-on-send enable command 125

neighbor-filter command 126
nsf (multicast) command 241
nsf lifetime (IGMP)nsf lifetime (IGMP/MLD) command 19
nsf lifetime (PIM) command 127

O

old-register-checksum command 128
oom-handling command 243
originator-id command 67

P

password (peer) command 68
peer (MSDP) command 70

Q

query-interval command 21
query-max-response-time command 23
query-timeout command 25

R

rate-per-route command 244
remote-as (multicast) command 71
robustness-count command 27
route-policy command 245
router command 28
router igmp command 30
router pim command 129
rp-address command 130
rp-static-deny command 136
rpf topology route-policy command 132
rpf-redirect command 133–134
rpf-vector command 137–138

S

sa-filter command 72
show auto-rp candidate-rp command 139
show igmp groups command 31
show igmp nsf command 33
show igmp nsr command 35
show igmp ssm map command 37
show igmp summary command 38
show igmp traffic command 41
show igmp vrf vrf_name groups command 44
show mfib connections command 247
show mfib counter command 249
show mfib encap-info command 251
show mfib interface command 252
show mfib nsf command 254
show mfib route command 256, 260
show mfib table-info command 262
show mrib client command 264
show mrib mpls forwarding command 267
show mrib mpls route command 269
show mrib nsf command 270
show mrib nsr command 76
show mrib nsr end command 272
show mrib route command 276
show mrib route outgoing-interface command 279
show mrib route-collapse command 274
show mrib table-info command 281
show mrib tlc command 283
show mrib vrf vrf_name route command 284
show msdp globals command 74
show msdp peer command 77
show msdp rpf command 79
show msdp sa-cache command 81
show msdp statistics peer command 85
show msdp summary command 87
show pim context command 149
show pim context table command 152
show pim global summary command 141
show pim group-map command 154
show pim interface command 156
show pim join-prune statistic command 159
show pim mstatic command 161
show pim neighbor command 163
show pim nsf command 143, 166
show pim range-list command 168
show pim rpf command 170
show pim rpf hash command 172
show pim rpf route-policy statistics command 174
show pim rpf route-policy test command 176
show pim rpf summary command 178
show pim rpf-redirect command 145–146
show pim segment-database command 147
show pim summary command 180
show pim topology command 182
show pim topology detail command 188
show pim topology entry-flag command 191
show pim topology interface-flag command 193
show pim topology summary command 195
show pim traffic command 197
show pim tunnel info command 199
show pim vrf vrf_name rpf command 201
show pim vrf vrf_name topology command 202
shutdown (MSDP) command 89
spt-threshold infinity command 203
ssm command 204
ssm map static command 45
static-group command 46
static-rpf command 286

T

ttl-threshold (MSDP) command 92

V

version command 48
vrf (igmp) command 50
vrf (multicast) command 291