Cisco IOS XR Multicast Command Reference for the Cisco CRS Router, Release 5.1.x

First Published: 2013-09-01

Last Modified: 2014-04-01

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

CONTENTS

Preface

Preface xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

IGMP and MLD Commands on Cisco IOS XR Software 1

access-group (IGMP/MLD) 3

clear igmp counters 5

clear igmp group 7

clear igmp reset 9

clear mld counters 11

clear mld group 13

clear mld reset 15

explicit-tracking 17

join-group 19

maximum groups 21

maximum groups-per-interface 24

mLDP OAM 27

nsf lifetime (IGMP/MLD) 29

query-interval 31

query-max-response-time 33

query-timeout 35

robustness-count 37

router 38

router igmp 40

router mld 42

show igmp groups 44

show igmp interface 47

show igmp nsf 51

show igmp summary 53
show igmp ssm map 56
show igmp traffic 57
show mld groups 61
show mld interface 63
show mld nsf 66
show mld ssm map 68
show mld summary 69
show mld traffic 71
ssm map 73
static-group 75
version 77
vrf (igmp) 79

CHAPTER 2 Multicast Source Discovery Protocol Commands 81
cache-sa holdtime 83
cache-sa-state 84
clear msdp peer 86
clear msdp sa-cache 87
clear msdp stats 89
connect-source 91
default-peer 93
description (peer) 95
maximum external-sa 97
maximum peer-external-sa 99
mesh-group (peer) 101
originator-id 103
password (peer) 104
peer (MSDP) 106
remote-as (multicast) 108
sa-filter 109
show msdp globals 111
show msdp peer 114
show msdp rpf 117
show msdp sa-cache 119

show msdp statistics peer 124
show msdp summary 126
shutdown (MSDP) 128
ttl-threshold (MSDP) 129

CHAPTER 3 Multicast Routing and Forwarding Commands 131
accounting per-prefix 133
accounting per-prefix forward-only 135
address-family (multicast) 137
boundary 140
clear mfib counter 142
clear mfib database 144
clear mfib hardware resource-counters 145
clear mfib hardware route statistics 147
disable (multicast) 150
enable (multicast) 152
forwarding-latency 154
interface (multicast) 155
interface all enable 157
interface-inheritance disable 159
log-traps 161
maximum disable 162
mdt data 163
mdt data ingress replication 165
mdt default 166
mdt mtu 168
mdt source 170
multicast-routing 172
multipath 174
nsf (multicast) 176
oom-handling 178
rate-per-route 180
show mfib connections 181
show mfib counter 183
show mfib encap-info 185

show mfib hardware interface 187
show mfib hardware resource-counters 190
show mfib hardware route accept-bitmap 193
show mfib hardware route olist 197
show mfib hardware route statistics 200
show mfib hardware route summary 203
show mfib hardware session-info 205
show mfib interface 207
show mfib mdt statistics 210
show mfib nsf 211
show mfib route 214
show mfib table-info 218
show mrib client 221
show mrib fgid 224
show mrib label-table-info 230
show mrib mdt-interface 231
show mrib nsf 233
show mrib route 235
show mrib route-collapse 239
show mrib route outgoing-interface 241
show mrib table-info 243
show mrib tlc 245
static-rpf 247
ttl-threshold (multicast) 249
vrf (multicast) 251

CHAPTER 4 Multicast PIM Commands 253

accept-register 256
auto-rp candidate-rp 257
auto-rp listen disable 260
auto-rp mapping-agent 261
bsr-border 263
bsr candidate-bsr 264
bsr candidate-rp 266
clear pim autorp 268

clear pim bsr 270
clear pim counters 272
clear pim topology 275
dr-priority 277
embedded-rp 279
global maximum 282
global maximum bsr crp-cache threshold 284
hello-interval (PIM) 286
interface (PIM) 288
interface all disable 290
join-prune-interval 291
join-prune-mtu 293
maximum autorp mapping-agent-cache 294
maximum group-mappings autorp 296
maximum register-states 298
maximum route-interfaces 299
maximum routes 300
mofrr 301
neighbor-check-on-recv enable 304
neighbor-check-on-send enable 305
neighbor-filter 306
nsf lifetime (PIM) 307
old-register-checksum 309
router pim 311
rp-address 313
rpf topology route-policy 315
rpf-redirect 317
rpf-redirect bundle 318
rpf-vector 320
rp-static-deny 321
show auto-rp candidate-rp 322
show auto-rp mapping-agent 324
show pim bgp-safi 326
show pim bsr candidate-rp 328
show pim bsr election 330

show pim bsr rp-cache 332
show pim context 334
show pim context detail 337
show pim context table 341
show pim df election-state 343
show pim df winner 346
show pim global summary 348
show pim group-map 350
show pim interface 353
show pim join-prune statistic 356
show pim rpf-redirect 358
show pim rpf-redirect route 360
show pim mdt 361
show pim mstatic 363
show pim neighbor 365
show pim nsf 368
show pim range-list 370
show pim rpf 372
show pim rpf hash 374
show pim rpf route-policy statistics 377
show pim rpf route-policy test 379
show pim rpf summary 381
show pim summary 383
show pim table-context 385
show pim topology 387
show pim topology detail 393
show pim topology entry-flag 396
show pim topology interface-flag 399
show pim topology summary 402
show pim traffic 404
show pim tunnel info 407
spt-threshold infinity 409
ssm 410

CHAPTER 5 Multicast Tool and Utility Commands 413

mrinfo 414

mtrace 416

sap cache-timeout 418

sap listen 419

show sap 421

CHAPTER 6 Automatic Multicast Tunneling Commands 425

advertisement-address 426

clear mfib counter amt 427

gateway-filter 428

maximum gateway 429

maximum route 430

maximum route-gateway 431

mtu (amt) 432

router amt relay ipv4 433

qqic 434

show amt gateway 435

show amt summary 436

show mrib amt gateway 437

show mrib amt route 440

tos(amt) 442

ttl(amt) 443

Preface

The Preface contains these topics:

- Obtaining Documentation and Submitting a Service Request, page xi

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

IGMP and MLD Commands on Cisco IOS XR Software

This chapter describes the commands used to configure and monitor IPv4 and IPv6 protocol using Cisco IOS XR Software .

The commands in this chapter apply to these protocols:

- Internet Group Management Protocol (IGMP) (Versions 1, 2, and 3)
- Multicast Listener Discovery (MLD) Protocol (Versions 1 and 2)

Note IGMP Versions 2 and 3 are equivalent to MLD Versions 1 and 2.

IGMP Version 1 does not have a complementary MLD version.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the Implementing Multicast Routing on Cisco IOS XR Software configuration module in *Cisco IOS XR Multicast Configuration Guide for the Cisco CRS Router* .

- access-group (IGMP/MLD), page 3
- clear igmp counters, page 5
- clear igmp group, page 7
- clear igmp reset, page 9
- clear mld counters, page 11
- clear mld group, page 13
- clear mld reset, page 15
- explicit-tracking, page 17
- join-group, page 19
- maximum groups, page 21
- maximum groups-per-interface, page 24
- mLDP OAM, page 27

- nsf lifetime (IGMP/MLD) , page 29
- query-interval, page 31
- query-max-response-time, page 33
- query-timeout, page 35
- robustness-count, page 37
- router, page 38
- router igmp, page 40
- router mld, page 42
- show igmp groups, page 44
- show igmp interface, page 47
- show igmp nsf, page 51
- show igmp summary, page 53
- show igmp ssm map, page 56
- show igmp traffic, page 57
- show mld groups, page 61
- show mld interface, page 63
- show mld nsf, page 66
- show mld ssm map, page 68
- show mld summary, page 69
- show mld traffic, page 71
- ssm map, page 73
- static-group, page 75
- version, page 77
- vrf (igmp), page 79

access-group (IGMP/MLD)

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

MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for MLD Protocol (Versions 1 and 2).

Usage Guidelines

If this command is not specified in router Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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 GigabitEthernet interface 0/1/0/1 can join only group 225.2.2.2:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 access-list mygroup permit 225.2.2.2 0.0.0.0
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface GigE 0/1/0/1
RP/0/RP0/CPU0:router(config-igmp-default-if)# access-group mygroup
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 access-list mygroup permit 225.2.2.2 0.0.0.0
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface GigE 0/1/0/1
RP/0/RP0/CPU0:router(config-igmp-default-if)# access-group mygroup
```

In the following example, an access group is configured for IPv6:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 access-list mld-acl
RP/0/RP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 any host ff3e::8000:1bb8
RP/0/RP0/CPU0:router(config-ipv6-acl)# exit
RP/0/RP0/CPU0:router(config)# router mld
RP/0/RP0/CPU0:router(config-mld)# access-group mld-acl
```

Related Commands

Command	Description
ipv4 access-list	Defines a standard IP access list. For information, see *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router*

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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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:

```
RP/0/RP0/CPU0: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

RP/0/RP0/CPU0:router# clear igmp counters

RP/0/RP0/CPU0: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 57	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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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 groups** 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.

```
RP/0/RP0/CPU0:router# show igmp groups tenGigE 0/4/0/0

IGMP Connected Group Membership
Group Address   Interface                 Uptime    Expires   Last Reporter
224.0.0.2       TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.5       TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.6       TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.13      TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.22      TenGigE0/4/0/0            3w6d      never     10.114.8.44

RP/0/RP0/CPU0:router# clear igmp groups tenGigE 0/4/0/0

RP/0/RP0/CPU0:router# show igmp groups tenGigE 0/4/0/0

IGMP Connected Group Membership
Group Address   Interface                 Uptime    Expires   Last Reporter
224.0.0.2       TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.5       TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.6       TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.13      TenGigE0/4/0/0            3w6d      never     10.114.8.44
224.0.0.22      TenGigE0/4/0/0            3w6d      never     10.114.8.44
```

Related Commands

Command	Description
show igmp groups, on page 44	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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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:

```
RP/0/RP0/CPU0:router# clear igmp reset
```

Related Commands

Command	Description
show igmp groups, on page 44	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.

clear mld counters

To clear Multicast Listener Discovery (MLD) traffic statistics, use the **clear mld counters** command in EXEC mode.

clear mld [**ipv6 vrf** *vrf-name*| **vrf** *vrf-name*] **counters**

Syntax Description

ipv6	(Optional) Specifies IPv6 addressing. IPv6 is the default for MLD 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 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

After MLD statistics are cleared, statistics begin incrementing once again.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows how to clear MLD traffic statistics:

```
RP/0/RP0/CPU0:router# clear mld counters
```

Note See the **clear igmp counters** command examples for complete output.

Related Commands

Command	Description
show mld traffic, on page 71	Displays all the Multicast Listener Discovery (MLD) traffic-related counters.

clear mld group

To clear Multicast Listener Discovery (MLD) groups on one or all interfaces, use the **clear mld group** command in EXEC mode.

clear mld [**ipv6 vrf** *vrf-name*| **vrf** *vrf-name*] **group** [*type path-id*]

Syntax Description

ipv6	(Optional) Specifies IPv6 addressing. IPv6 is the default for MLD groups.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
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 no group address is specified, all MLD groups are cleared.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **clear mld group** command is used to clear user-specified MLD membership or all MLD membership learned from external hosts. Use the *type* and *number* arguments to clear specific MLD membership, or if no interface arguments are specified, clear MLD membership from all interfaces. This command does not clear local static group members.

Task ID

Task ID	Operations
multicast	execute

Examples

The following example shows how to clear MLD groups for Packet-over-SONET/SDH (POS) interface 0/4/0/0:

```
RP/0/RP0/CPU0:router# clear mld group pos 0/4/0/0
```

Note See the **clear igmp group** command examples for complete output.

Related Commands

Command	Description
clear igmp group, on page 7	Clears Internet Group Management Protocol (IGMP) groups on one or all interfaces.
show mld groups, on page 61	Displays the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD).

clear mld reset

To clear all Multicast Listener Discovery (MLD) membership entries and reset connection in the Multicast Routing Information Base (MRIB), use the **clear mld reset** command in EXEC mode.

clear mld [**ipv6 vrf** *vrf-name*| **vrf** *vrf-name*] **reset**

Syntax Description

ipv6	(Optional) Specifies IPv6 addressing. IPv6 is the default for MLD 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 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

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

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

Note This command is reserved to force synchronization of MLD 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:

```
RP/0/RP0/CPU0:router# clear igmp mld reset
```

Related Commands

Command	Description
show mld groups, on page 61	Displays the multicast groups that are directly connected to the router and that were learned through MLD.
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 or Multicast Listener Discovery (MLD) Version 2, 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 or MLD configuration mode, then explicit host tracking is disabled.

Command Modes

IGMP VRF configuration

IGMP interface configuration

MLD configuration

MLD interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	The **enable** keyword was removed. The **disable** keyword was removed from IGMP and MLD configuration modes.

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 or MLD membership of hosts, use the **show igmp groups** or the **show mld 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 or MLD configuration mode, parameters are inherited by all new and existing interfaces. However, you can override these parameters on individual interfaces from IGMP or router MLD 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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# explicit-tracking router1
RP/0/RP0/CPU0:router(config-igmp)# interface GigabitEthernet 0/1/0/0
RP/0/RP0/CPU0:router(config-igmp-default-if)# explicit-tracking disable
```

Related Commands

Command	Description
show igmp groups, on page 44	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).
show mld groups, on page 61	Displays the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD).

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 either IPv4 or IPv6 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* . • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X* .
source-address	(Optional) Source address of the multicast group to include in either IPv4 or IPv6 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* . • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X* .

Command Default

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

Command Modes

IGMP interface configuration

MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for Multicast Listener Discovery (MLD) Protocol (Versions 1 and 2).
Release 3.5.0	The **include** *include-address* and **exclude** *exclude-address* keywords and arguments have been removed.

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 or MLD 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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface GigabitEthernet 0/1/0/0
RP/0/RP0/CPU0:router(config-igmp-default-if)# join-group 225.2.2.2
```

Related Commands

Command	Description
ping	Checks host reachability and network connectivity on IP networks. For information, see *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router*.

maximum groups

To configure the maximum number of groups used by Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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

MLD configuration

MLD VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for MLD Protocol (Versions 1 and 2).

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.

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:

```
RP/0/RP0/CPU0: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-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
GigabitEthernet0/1/5/0   3         25000
GigabitEthernet0/1/5/1   5         25000
GigabitEthernet0/1/5/2   5         25000
POS0/1/0/1               5         25000
POS0/1/4/2               3         25000
GigabitEthernet0/6/5/1   3         25000
GigabitEthernet0/6/5/2   3         25000
GigabitEthernet0/6/5/7   3         25000
POS0/6/0/1               3         25000
POS0/6/4/4               3         25000
POS0/6/4/5               3         25000
POS0/6/4/6               3         25000

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# maximum groups 10
RP/0/RP0/CPU0:router(config-igmp)# commit

% Failed to commit one or more configuration items during an atomic operation, n
o changes have been made. Please use 'show configuration failed' to view the errors

RP/0/RP0/CPU0:router# show configuration failed

[!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
router igmp
maximum groups 10
!!% Invalid argument: The desired new maximum for the number of groups 10 must be equal or
 larger than the present number of groups, which is 61

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router igmp
```

```
RP/0/RP0/CPU0:router(config-igmp)# maximum groups 65
RP/0/RP0/CPU0:router(config-igmp)# commit

RP/0/RP0/CPU0:routerMay 13 12:26:59.108 : config[65704]: %LIBTARCFG-6-COMMIT : Configuration
 committed
by user 'cisco'. Use 'show commit changes 1000000025' to view the changes.

RP/0/RP0/CPU0: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         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
GigabitEthernet0/1/5/0     3         25000
GigabitEthernet0/1/5/1     5         25000
GigabitEthernet0/1/5/2     5         25000
POS0/1/0/1                 5         25000
POS0/1/4/2                 3         25000
GigabitEthernet0/6/5/1     3         25000
GigabitEthernet0/6/5/2     3         25000
GigabitEthernet0/6/5/7     3         25000
POS0/6/0/1                 3         25000
POS0/6/4/4                 3         25000
POS0/6/4/5                 3         25000
POS0/6/4/6                 3         25000
```

Related Commands

Command	Description
maximum groups-per-interface, on page 24	Configures the maximum number of groups for each interface accepted by a router.
show igmp summary, on page 53	Displays group membership information for Internet Group Management Protocol (IGMP).
show mld summary, on page 69	Displays group membership information for Multicast Listener Discovery (MLD).

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

Router MLD configuration

Router MLD VRF configuration

Router MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for Multicast Listener Discovery (MLD) Protocol (Versions 1 and 2).
Release 3.5.0	The command was changed from **maximum groups per-interface** to **maximum groups-per-interface** .

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 or MLD 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:

```
RP/0/RP0/CPU0: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
GigabitEthernet0/1/5/0   3         25000
GigabitEthernet0/1/5/1   5         25000
GigabitEthernet0/1/5/2   5         25000
GigabitEthernet0/6/5/1   3         25000
GigabitEthernet0/6/5/2   3         25000
GigabitEthernet0/6/5/7   3         25000

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# maximum groups-per-interface 5
RP/0/RP0/CPU0:router(config-igmp)# commit


RP/0/RP0/CPU0: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
GigabitEthernet0/1/5/0     3          5
GigabitEthernet0/1/5/1     5          5
GigabitEthernet0/1/5/2     5          5
GigabitEthernet0/6/5/1     3          5
GigabitEthernet0/6/5/2     3          5
GigabitEthernet0/6/5/7     3          5
```

The following example shows how to configure all interfaces with 3000 maximum groups per interface except Packet-over-SONET/SDH (POS) interface 0/4/0/0, which is set to 4000:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# maximum groups-per-interface 3000
RP/0/RP0/CPU0:router(config-igmp)# interface POS 0/4/0/0
RP/0/RP0/CPU0:router(config-igmp-default-if)# maximum groups-per-interface 4000
```

Related Commands

Command	Description
maximum groups, on page 21	Configures the maximum number of groups used by Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) .
show igmp summary, on page 53	Displays group membership information for Internet Group Management Protocol (IGMP).

mLDP OAM

To add OAM functions to mLDP, use the **mLDP OAM** command.

To execute ping or trace for a specified mLDP tree, use the **ping mpls mldp** and **trace mpls mldp** commands in the global configuration mode.

ping mpls mldp[**p2mp**|**mp2mp**] *root opaque_types* [*options*]

trace mpls mldp[**p2mp**|**mp2mp**] *root opaque_types* [*options*]

Both commands use the same syntax.

Syntax Description

p2mp|**mp2mp**	Type of tree on which the ping is performed.
root	Address of the root in the tree.
opaque_types	Set of opaque types and their subsequent parameters : • ipv4 <rd> <source> <group> [options] • ipv6 <rd> <source> <group> [options] • hex <opaque type> <opaque value> [options] • mdt <vpnid> <mdt_num> [options] • global-id <global identifier> [options]
options	Regular ping/trace options.

Command Default

No default behavior or values.

Command Modes

Global configuration mode.

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
mpls	read, write

Examples

```
RP/0/RP0/CPU0:router(config)# ping mpls mldp p2mp ipv4
RP/0/RP0/CPU0:router(config)# trace mpls mldp p2mp ipv4
```

nsf lifetime (IGMP/MLD)

To configure the maximum time for the nonstop forwarding (NSF) timeout on the Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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

MLD configuration

MLD VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for MLD Protocol (Versions 1 and 2).

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 Auto-RP and the Session Announcement Protocol (SAP) Listener) and updates the MRIB.

Note The NSF process for MLD under IPv6 is as described above for IGMP under IPv4.

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/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(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.
show igmp nsf, on page 51	Displays the state of NSF operation in IGMP.
show mfib nsf	Displays the state of NSF operation for the MFIB line cards.
show mld nsf, on page 66	Displays the state of NSF operation in MLD.

query-interval

To configure the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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 or MLD configuration mode.

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

Command Modes

IGMP VRF configuration

IGMP interface configuration

MLD configuration

MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for MLD Protocol (Versions 1 and 2).

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 or MLD 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 or MLD 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, and MLD Versions 1 and 2, 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 or MLD 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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface gigabitEthernet

0/1/0/0
RP/0/RP0/CPU0: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 44	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show mld groups, on page 61	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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 or MLD 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 or MLD configuration mode.

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

Command Modes

IGMP VRF configuration

IGMP interface configuration

MLD configuration

MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for MLD Protocol (Versions 1 and 2).

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 or MLD 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 or MLD 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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RP0/CPU0: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 44	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show mld groups, on page 61	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

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

MLD configuration

MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	Support was added for Multicast Listener Discovery (MLD) Protocol (Versions 1 and 2).

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 or MLD 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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RP0/CPU0:router(config-igmp-default-if)# query-timeout 30
```

Related Commands

Command	Description
query-interval, on page 31	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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

MLD configuration

MLD interface configuration

Command History

Release	Modification
Release 3.6.0	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/RP0/CPU0:router(config)# configure
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# robustness-count 2
```

router

To disable or enable Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) 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 or MLD membership tracking.
enable	Turns on IGMP or MLD 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

MLD interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **router** command is used to enable and disable the IGMP or MLD router functionality on a specific interface. For instance, IGMP or MLD stops queries from an interface when the router functionality is disabled on that interface. Disabling IGMP or MLD 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 or MLD 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 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RP0/CPU0: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 2.0	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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)#
```

Related Commands

Command	Description
interface all disable	Disables IGMP or MLD 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.

router mld

To enter router Multicast Listener Discovery (MLD) Protocol configuration mode, use the **router mld** command in
global

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

router mld

no router mld

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 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enter MLD configuration mode:

```
RP/0/RP0/CPU0:router(config)# router mld
RP/0/RP0/CPU0:router(config-mld)#
```

Related Commands

Command	Description
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 [old-output] [**vrf** *vrf-name*] **groups** [*group-address*| *type interface-path-id*| **not-active**| **summary**] **[detail] [explicit]**

Syntax Description

old-output	(Optional) Displays the previous show output—available for backward compatibility.
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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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 (tenGigE) interface:

```
RP/0/RP0/CPU0:router# show igmp groups tenGigE 0/4/0/0

IGMP Connected Group Membership
Group Address   Interface                Uptime    Expires   Last Reporter
224.0.0.2       TenGigE0/4/0/0           3w6d      never     10.114.8.44
224.0.0.5       TenGigE0/4/0/0           3w6d      never     10.114.8.44
224.0.0.6       TenGigE0/4/0/0           3w6d      never     10.114.8.44
224.0.0.13      TenGigE0/4/0/0           3w6d      never     10.114.8.44
224.0.0.22      TenGigE0/4/0/0           3w6d      never     10.114.8.44
```

This table describes the significant fields shown in the display.

Table 1: 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.

Related Commands

Command	Description
show igmp interface, on page 47	Displays Internet Group Management Protocol (IGMP) multicast-related information about an interface.

show igmp interface

To display Internet Group Management Protocol (IGMP) multicast-related information about an interface, use the **show igmp interface** command in EXEC mode.

show igmp [old-output] [**vrf** *vrf-name*] **interface** [*type inteface-path-id*| **state-on**| **state-off**]

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.
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.
state-on	(Optional) Displays all interfaces with IGMP enabled.
state-off	(Optional) Displays all interfaces with IGMP disabled.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If you omit the optional arguments, the **show igmp interface** command displays information about all interfaces.

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# show igmp interface

Loopback0 is up, line protocol is up
  Internet address is 10.144.144.144/32
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 3 joins, 0 leaves
  IGMP querying router is 10.144.144.144 (this system)
TenGigE0/4/0/0 is up, line protocol is up
  Internet address is 10.114.8.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 9 joins, 4 leaves
  IGMP querying router is 10.114.8.11
Bundle-Ether16.162 is up, line protocol is up
  Internet address is 10.194.8.44/24
  IGMP is disabled on interface
Bundle-Ether16.163 is up, line protocol is up
  Internet address is 10.194.12.44/24
  IGMP is disabled on interface
GigabitEthernet0/1/0/2 is up, line protocol is up
  Internet address is 10.147.4.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 6 joins, 0 leaves
  IGMP querying router is 10.147.4.44 (this system)
GigabitEthernet0/1/0/8 is up, line protocol is up
  Internet address is 10.146.4.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 5 joins, 0 leaves
  IGMP querying router is 10.146.4.44 (this system)
GigabitEthernet0/1/0/18 is up, line protocol is up
  Internet address is 10.194.4.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 7 joins, 2 leaves
  IGMP querying router is 10.194.4.19
GigabitEthernet0/1/0/23 is up, line protocol is up
  Internet address is 10.114.4.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
```

```
  IGMP activity: 9 joins, 4 leaves
  IGMP querying router is 10.114.4.11
GigabitEthernet0/1/0/27 is up, line protocol is up
  Internet address is 10.145.4.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 7 joins, 2 leaves
  IGMP querying router is 10.145.4.44 (this system)
```

This table describes the significant fields shown in the display.

Table 2: show igmp interface Field Descriptions

Field	Description
Loopback0 is up, line protocol is up	Interface type, number, and status.
Internet address is	Internet address of the interface and subnet mask being applied to the interface, as specified with the **address** command.
IGMP is enabled on interface	Indicates whether IGMP router functionality has been enabled on the interface. **Note** Multicast protocols do not run on Management Ethernet interfaces even if they are enabled with the CLI.
IGMP query interval is 60 seconds	Interval at which the Cisco IOS XR software software sends Protocol Independent Multicast (PIM) query messages, as specified with the **query-interval** command.
IGMP querier timeout is...	Timeout that is set by nonquerier routers. When this timeout expires, the nonquerier routers begin to send queries.
IGMP max query response time is...	Query response time, in seconds, that is used by administrators to tune the burstiness of IGMP messages on the network. This is the maximum time within which a response to the query is received.
Last member query response is...	Query response time in seconds since a host replied to a query that was sent by the querier.
IGMP activity:	Total number of joins and total number of leaves received.
IGMP querying router is 239.122.41.51 (this system)	Indicates the elected querier on the link.

Related Commands

Command	Description
address	Sets a primary or secondary IP address for an interface.
query-interval, on page 31	Configures the frequency at which Cisco IOS XR software sends IGMP host-query messages.
router, on page 38	Disables or enables MLD or IGMP membership tracking.

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 [old-output] [**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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# show igmp nsf

IP IGMP Non-Stop Forwarding Status
:
 Multicast routing state: Non-Stop Forwarding Activated

NSF Lifetime: 00:01:00
```

```
NSF
Time Remaining:       00:
00:
06
```

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).
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/MLD) , on page 29	Configures the NSF timeout value for the IGMP or MLD 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 summary

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

show igmp [old-output] [**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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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:

```
RP/0/RP0/CPU0: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
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

GigabitEthernet0/1/5/0    3         5

GigabitEthernet0/1/5/1

5         5

GigabitEthernet0/1/5/2

5         5

POS0/1/0/1

5         5

POS0/1/4/2                3         5

GigabitEthernet0/
6/
5/
1

 3         5
GigabitEthernet0/
6/5/
2    3         5
GigabitEthernet0/
6/5/
7

3         5

POS0/
6/
0/
1

3         5

POS0/6/
4/
4                3         5

POS0/6/
```

```
4/
5                   3           5

POS0/6/
4/
6                   3           5
```

This table describes the significant fields shown in the display.

Table 4: 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.
Disabled Interfaces	Number of disabled interfaces.

Related Commands

Command	Description
show igmp groups, on page 44	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

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 3.7.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# show igmp ssm map 232.1.1.1

232.1.1.1 is static with 1 source
```

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 [old-output] [**vrf vrf-name**] **traffic**

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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 both the **show igmp traffic** and **show mld traffic** command, since they are identical. For information about the **show mld traffic** command, see show mld traffic, on page 71

Table 5: show igmp traffic and show mld traffic Field Descriptions

Field	Description
Valid IGMP/MLD 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 that a neighboring interface no longer has multicast reception state for a particular group.
Mtrace packets	(IGMP only) Total number of Mtrace packets sent and received. Mtrace traces the route from a receiver to a source using a particular multicast address.

Field	Description
DVMRP packets	(IGMP only) 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	(IGMP only) 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. **Note** MLD checksum verification is performed by the ICMPv6 protocol; this counter, therefore, never increments in MLD.
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.
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.

Field	Description
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 mld traffic, on page 71	Displays all the Multicast Listener Discovery (MLD) traffic-related counters.

show mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the **show mld groups** command in EXEC mode .

show mld [old-output] [**vrf** *vrf-name*] **groups** [*group-address*| *type path-id*| **not-active**| **summary**] **[detail] [explicit]**

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.
group-address	(Optional) Name or address of the multicast group. Name is as defined in the Domain Name System (DNS) hosts table. Address is a multicast IP address in IPv6 format.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
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.
not-active	(Optional) Displays group joins that are not processed.
summary	(Optional) Displays the total number of (* , G) and (S, G) states in MLD.
detail	(Optional) Displays detail information such as MLD 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 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If you omit all optional arguments, the **show mld 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 mld groups** command:

```
RP/0/RP0/CPU0:router# show mld groups

MLD Connected Group Membership

POS0/2/0/0

Group Address : ff02::2
Last Reporter : fe80::b000:ff:fe00:fb00
       Uptime : 01:56:39
      Expires : never
Group Address : ff02::d
Last Reporter : fe80::b000:ff:fe00:fb00
       Uptime : 01:56:39
      Expires : never
Group Address : ff02::16
Last Reporter : fe80::b000:ff:fe00:fb00
       Uptime : 01:56:39
      Expires : never
```

Table 1: show igmp groups Field Descriptions, on page 45 describes the significant fields shown in the display.

Related Commands

Command	Description
show mld interface, on page 63	Displays Multicast Listener Discovery (MLD) multicast-related information about an interface.

show mld interface

To display Multicast Listener Discovery (MLD) multicast-related information about an interface, use the **show mld interface** command in EXEC mode .

show mld [old-output] [**vrf** *vrf-name*] **interface** [*type path-id*| **state-on**| **state-off**]

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.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
instance	(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 all interfaces with IGMP enabled.
state-off	(Optional) Displays all interfaces with IGMP disabled.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If you omit the optional arguments, the **show mld interface** command displays information about all interfaces.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mld interface** command:

```
RP/0/RP0/CPU0:router# show mld interface

Loopback0 is up, line protocol is up
  Internet address is fe80::5000:ff:fe00:5c00
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  MLD activity: 3 joins, 0 leaves
  MLD querying router is fe80::5000:ff:fe00:5c00 (this system)
TenGigE0/5/0/2 is up, line protocol is up
  Internet address is fe80::215:c6ff:fe3e:8c85
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  MLD activity: 5 joins, 0 leaves
  MLD querying router is fe80::215:c6ff:fe3e:8c85 (this system)
TenGigE0/5/0/3 is up, line protocol is up
  Internet address is fe80::215:c6ff:fe3e:8c86
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  MLD activity: 5 joins, 0 leaves
  MLD querying router is fe80::215:c6ff:fe3e:8c86 (this system)
TenGigE0/5/0/3.4 is up, line protocol is up
  Internet address is fe80::215:c6ff:fe3e:8c86
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  MLD activity: 3 joins, 0 leaves
  MLD querying router is fe80::215:c6ff:fe3e:8c86 (this system)
TenGigE0/5/0/3.5 is up, line protocol is up
  Internet address is fe80::215:c6ff:fe3e:8c86
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  MLD activity: 3 joins, 0 leaves
  MLD querying router is fe80::215:c6ff:fe3e:8c86 (this system)
```

Table 2: show igmp interface Field Descriptions, on page 49 describes the significant fields shown in the display.

Related Commands

Command	Description
address	Sets a primary or secondary IP address for an interface.

Command	Description
query-interval, on page 31	Configures the frequency at which Cisco IOS XR Software sends MLD host-query messages.
router, on page 38	Disables or enables MLD or IGMP membership tracking.

show mld nsf

To display the state of the nonstop forwarding (NSF) operation in Multicast Listener Discovery (MLD), use the **show mld nsf** command in EXEC mode .

show mld [old-output] [**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 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show mld nsf** command displays the current multicast NSF state for MLD. 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 MLD 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 mld nsf** command:

```
RP/0/RP0/CPU0:router# show mld nsf

IP MLD Non-Stop Forwarding Status:
Multicast routing state: Non-Stop Forwarding Activated
NSF Lifetime: 00:01:00
NSF Time Remaining: 00:00:06
```

Table 3: show igmp nsf Field Descriptions, on page 52 describes the significant fields shown in the display.

Related Commands

Command	Description
nsf (multicast)	Enables NSF capability for the multicast routing system.
nsf lifetime (IGMP/MLD) , on page 29	Configures the NSF timeout value for the IGMP or MLD 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 mld ssm map

To display the source-specific mapping (SSM) state in Multicast Listener Discovery (MLD), use the **show mld ssm map** command in EXEC mode.

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

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
group-address	(Optional) 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 3.7.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# show mld ssm map 2001:0DB8::/48

2001:0DB8::/48 is static with 1 source
```

show mld summary

To display group membership information for Multicast Listener Discovery (MLD), use the **show mld summary** command in EXEC mode.

show mld [old-output] [**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 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show mld 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 MLD members and the maximum number of groups that can become members on each interface:

```
RP/0/RP0/CPU0:router# show mld summary

MLD summary
```

```
Robustness Value 2
No. of Group x Interfaces 39
Maximum number of Group x Interfaces 4500

Supported Interfaces   : 12
Unsupported Interfaces : 1
Enabled Interfaces     : 2
Disabled Interfaces    : 3

Interface                Grp No    Max Grp No
Loopback0                11        25000
Loopback1                10        25000
Loopback2                9         25000
Loopback3                9         25000
```

Table 4: show igmp summary Field Descriptions, on page 55 describes the significant fields shown in the display.

Related Commands

Command	Description
show mld groups, on page 61	Displays the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD).

show mld traffic

To display all the Multicast Listener Discovery (MLD) traffic-related counters, use the **show mld traffic** command in EXEC mode.

show mld [old-output] [**vrf** *vrf-name*] **traffic**

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 3.2	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

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

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# show mld traffic

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

                                    Received        Sent
Valid MLD Packet                         10          10
```

```
Queries                                 2           2
Reports                                 8           8
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
```

Table 5: show igmp traffic and show mld traffic Field Descriptions, on page 58 describes the significant fields shown in the display.

Related Commands

Command	Description
show pim traffic	Displays PIM traffic counter information.

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

MLD configuration

Command History

Release	Modification
Release 3.7.0	This command was introduced.

Usage Guidelines

PIM-SSM requires the use of IGMPv3 (IPv4) or MLD (IPv6) to determine local memberships. Under normal operating conditions, IGMP and MLD discard 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:

```
RP/0/RP0/CPU0:router(config)# configuration
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# ssm map static 10.0.0.1 mc2
RP/0/RP0/CPU0: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 either IPv4 or IPv6 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* . • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X* .
inc-mask *mask*	(Optional) Specifies a mask for the increment range. This is an IP address expressed range in either IPv4 or IPv6 prefixing 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* . • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X* . **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 either IPv4 or IPv6 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* . • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X* .

Command Default

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

Command Modes

IGMP interface configuration

MLD interface configuration

Command History

Release	Modification
Release 3.3.0	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.

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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface GigE 0/1/0/0
RP/0/RP0/CPU0: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) or Multicast Listener Discovery (MLD) 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. Available for IGMP and MLD.
2	Specifies IGMP Version 2. Available for IGMP and MLD.
3	Specifies IGMP Version 3. Available for IGMP only.

Command Default

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

If this command is not specified in IGMP or MLD configuration mode, IGMP uses Version 3 and MLD uses Version 1.

Command Modes

IGMP configuration

IGMP VRF configuration

IGMP interface configuration

MLD configuration

MLD VRF configuration

MLD interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	This command was supported in the following configuration modes: • IGMP interface configuration • MLD interface configuration

Usage Guidelines

All routers on the subnet must be configured with the same version of IGMP or MLD. 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 or MLD 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 or MLD Version 1 or 2.

Note If you configure this command in IGMP or MLD 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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# version 3
```

Related Commands

Command	Description
query-max-response-time, on page 33	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) queries.
query-timeout, on page 35	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 and MLD 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

MLD configuration

Command History

Release	Modification
Release 3.7.0	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. Likewise, when you use the **vrf** command from the MLD routing configuration mode, you enter MLD VRF configuration submode.

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

Note Although the **vrf** command is available in MLD routing configuration submode, MLD does not support virtual routing and forwarding. Its function there is simply to allow both routing protocols to share the same configuration code.

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:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# vrf
vrf_1
RP/0/RP0/CPU0:router(config-igmp-vrf_1)#
```

Multicast Source Discovery Protocol Commands

This chapter describes the commands used to configure and monitor the Multicast Source Discovery Protocol (MSDP) on the Cisco IOS XR Software .

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the *Implementing Multicast Routing on the Cisco IOS XR Software* configuration module in *Cisco IOS XR Multicast Configuration Guide for the Cisco CRS Router*.

- cache-sa holdtime, page 83
- cache-sa-state, page 84
- clear msdp peer, page 86
- clear msdp sa-cache, page 87
- clear msdp stats, page 89
- connect-source, page 91
- default-peer , page 93
- description (peer), page 95
- maximum external-sa, page 97
- maximum peer-external-sa, page 99
- mesh-group (peer), page 101
- originator-id, page 103
- password (peer), page 104
- peer (MSDP), page 106
- remote-as (multicast), page 108
- sa-filter, page 109
- show msdp globals, page 111
- show msdp peer, page 114
- show msdp rpf , page 117
- show msdp sa-cache, page 119

- show msdp statistics peer, page 124
- show msdp summary, page 126
- shutdown (MSDP), page 128
- ttl-threshold (MSDP), page 129

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 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router
msdp
RP/0/RP0/CPU0:router(config-msdp)# cache-sa-holdtime
200
```

Related Commands

Command	Description
cache-sa-state, on page 84	Controls cache source-active (SA) state on a router.

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 2.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# MSDP
RP/0/RP0/CPU0:router(config-msdp)# cache-sa-state list 100
```

```
RP/0/RP0/CPU0:router(config-msdp)# exit
RP/0/RP0/CPU0:router(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 119	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

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 2.0	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/RP0/CPU0:router# clear msdp peer 224.15.9.8
```

Related Commands

Command	Description
peer (MSDP), on page 106	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 2.0	This command was introduced.
Release 3.5.0	The **ipv4** keyword was added.

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/RP0/CPU0:router# clear msdp sa-cache 224.5.6.7
```

Related Commands

Command	Description
show msdp sa-cache, on page 119	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 2.0	This command was introduced.
Release 3.5.0	The **ipv4** keyword was added.

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/RP0/CPU0:router# clear msdp stats peer 224.0.1.1
```

Related Commands

Command	Description
show msdp statistics peer, on page 124	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 2.0	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/RP0/CPU0:router(config)# interface loopback 0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1/24
RP/0/RP0/CPU0:router(config-if)# exit
RP/0/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(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 2.0	This command was introduced.
Release 3.5.0	The command was moved from MSDP peer configuration mode to MSDP configuration mode. The **prefix-list** keyword was removed.

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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# default-peer 172.16.12.0
```

Related Commands

Command	Description
peer (MSDP), on page 106	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 2.0	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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 10.0.5.4
RP/0/RP0/CPU0:router(config-msdp-peer)# description 10.0.5.4 router_at_customer_site_A
```

Related Commands

Command	Description
peer (MSDP), on page 106	Configures a Multicast Source Discovery Protocol (MSDP) peer.
show msdp peer, on page 114	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 2.0	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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 10.1.5.3
RP/0/RP0/CPU0:router(config-msdp-peer)# maximum external-sa 25000
```

Related Commands

Command	Description
maximum peer-external-sa, on page 99	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 126	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 3.2	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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# maximum peer-external-sa 27000
```

Related Commands

Command	Description
maximum external-sa, on page 97	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 126	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 2.0	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] or multiprotocol 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router msdp
```

```
RP/0/RP0/CPU0:router(config-msdp)# peer 10.0.5.4
RP/0/RP0/CPU0:router(config-msdp-peer)# mesh-group internal
```

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 2.0	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:

```
RP/0/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# originator-id GigE0/1/1/0
```

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 3.5.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 10.0.5.4
RP/0/RP0/CPU0:router(config-msdp-peer)# password encrypted a34bi5m
```

Related Commands

Command	Description
show msdp peer, on page 114	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 2.0	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 or multiprotocol BGP with the MSDP peer, as long as there is a BGP or multiprotocol 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 172.16.1.2
RP/0/RP0/CPU0:router(config-msdp-peer)#
```

Related Commands

Command	Description
default-peer , on page 93	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 2.0	This command was introduced.
Release 3.5.0	Support was added for the *as-number* 4-byte number range 1.0 to 65535.65535.

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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 172.16.5.4
RP/0/RP0/CPU0:router(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 2.0	This command was introduced.

Usage Guidelin

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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 131.107.5.4
RP/0/RP0/CPU0:router(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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 131.107.5.4
RP/0/RP0/CPU0:router(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 106	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 2.0	This command was introduced.
Release 5.0.0	This command was introduced.
Release 3.9.0	Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations.

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/RP0/CPU0:router# 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 6: 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.

Field	Description
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 114	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
show msdp sa-cache, on page 119	Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

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 2.0	This command was introduced.
Release 3.9.0	Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# 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 7: 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.

Field	Description
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 106	Configures a Multicast Source Discovery Protocol (MSDP) peer.
show msdp sa-cache, on page 119	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 2.0	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/RP0/CPU0:router# 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 8: 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.
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 2.0	This command was introduced.

Release	Modification
Release 3.9.0	Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations.

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/RP0/CPU0:router# 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, MBGP/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 9: 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.

Field	Description
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/RP0/CPU0:router# 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, MBGP/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 10: 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.
MBGP/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/RP0/CPU0:router# 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 11: 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/RP0/CPU0:router# 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, MBGP/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, MBGP/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, MBGP/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 84	Controls cache source-active (SA) state on a router.
peer (MSDP), on page 106	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 2.0	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/RP0/CPU0:router# 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 12: 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 89	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 2.0	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/RP0/CPU0:router# 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 13: 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 114	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
show msdp sa-cache, on page 119	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 2.0	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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 172.16.5.4
RP/0/RP0/CPU0:router(config-msdp-peer)# shutdown
```

Related Commands

Command	Description
show msdp peer, on page 114	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.

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 2.0	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/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# ttl-threshold 8
```

Related Commands

Command	Description
peer (MSDP), on page 106	Configures a Multicast Source Discovery Protocol (MSDP) peer.

Multicast Routing and Forwarding Commands

This module describes the commands used to configure and monitor multicast routing.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the *Implementing Multicast Routing on Cisco IOS XR Software* configuration module in the *Cisco IOS XR Multicast Configuration Guide for the Cisco CRS Router*.

- accounting per-prefix, page 133
- accounting per-prefix forward-only, page 135
- address-family (multicast), page 137
- boundary, page 140
- clear mfib counter, page 142
- clear mfib database, page 144
- clear mfib hardware resource-counters, page 145
- clear mfib hardware route statistics, page 147
- disable (multicast), page 150
- enable (multicast), page 152
- forwarding-latency, page 154
- interface (multicast), page 155
- interface all enable, page 157
- interface-inheritance disable, page 159
- log-traps, page 161
- maximum disable, page 162
- mdt data, page 163
- mdt data ingress replication, page 165
- mdt default, page 166
- mdt mtu, page 168
- mdt source, page 170

- multicast-routing, page 172
- multipath, page 174
- nsf (multicast) , page 176
- oom-handling, page 178
- rate-per-route, page 180
- show mfib connections, page 181
- show mfib counter, page 183
- show mfib encap-info , page 185
- show mfib hardware interface, page 187
- show mfib hardware resource-counters, page 190
- show mfib hardware route accept-bitmap, page 193
- show mfib hardware route olist, page 197
- show mfib hardware route statistics, page 200
- show mfib hardware route summary, page 203
- show mfib hardware session-info, page 205
- show mfib interface, page 207
- show mfib mdt statistics, page 210
- show mfib nsf, page 211
- show mfib route, page 214
- show mfib table-info, page 218
- show mrib client, page 221
- show mrib fgid, page 224
- show mrib label-table-info, page 230
- show mrib mdt-interface, page 231
- show mrib nsf, page 233
- show mrib route, page 235
- show mrib route-collapse, page 239
- show mrib route outgoing-interface, page 241
- show mrib table-info, page 243
- show mrib tlc, page 245
- static-rpf, page 247
- ttl-threshold (multicast), page 249
- vrf (multicast), page 251

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 and IPv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

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, every existing and new (S, G) route is assigned forward, punt, and drop counters on the ingress route and forward and punt counters on the egress route. The (*, G) routes are assigned a single 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.

Because the use of this counter can be resource-intensive when a large number of routes are configured, such as for multicast VPN (there is a limit of 150,000 routes to a router), use the show mfib hardware resource-counters, on page 190 command in EXEC mode to check resource allocation. Should hardware resource allocation be an issue, we recommend the use of the accounting per-prefix forward-only, on page 135 command.

To verify the number of statistics allocated or free on a line card, use the show mfib hardware resource-counters, on page 190 command in EXEC mode.

You may switch between **accounting-perprefix** and **accounting per-prefix forward-only** statistics on any (S,G) route. However, be aware that only one set of counters is supported on the (*,G) routes (with fwd/punt/drop on ingress and fwd/drop on egress) regardless of whether you enabled the **accounting-perprefix** or **accounting-perprefix fwd-only** command.

Although you can switch accouting modes, this involves freeing the hardware statistics and reallocating them, thereby resulting in a loss of any previously collected data. Therefore, it is preferable to decide which statistics mode you want to use at the start to avoid the resource cost entailed by resetting the statistics counter values with a change in mode.

To display packet statistics, use the **show mfib route** and the **show mfib hardware route statistics** commands. These commands display "N/A" for counters when no hardware statistics are available or when neither the **accounting per-prefix** command nor the accounting per-prefix forward-only, on page 135 command is enabled.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable accounting for multicast routing:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# accounting per-prefix
```

Related Commands

Command	Description
accounting per-prefix forward-only, on page 135	Reduces hardware statistics resource allocations when enabling accounting, particularly for multicast VPN (MVPN).
show mfib hardware route statistics, on page 200	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

accounting per-prefix forward-only

To reduce hardware statistics resource allocations when enabling accounting, particularly for multicast VPN (MVPN), use the **accounting per-prefix forward-only** command under multicast routing configuration mode. To return to the default mode of accounting per-prefix, on page 133, use the **no** form of this command.

accounting per-prefix forward-only

no accounting per-prefix forward-only

Syntax Description

This command has no keywords or arguments.

Command Default

If no counters were configured, there is no default.

If the accounting per-prefix counter was previously configured, it becomes the default.

If no accounting was configured for multicast routing, forwarding-only is the default mode and triggers a data MDT transition in the case of MVPN deployment.

Command Modes

Multicast routing configuration

Multicast routing address family IPv4 and IPv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

Note The **accounting per-prefix forward-only** command has only one *fwd-only* counter. In other words, there is no *punt* or *drop* counter allocated.

We recommended this command for configuration of multicast VPN routing or for any line card that has a route-intensive configuration. Each individual router can support up to 150,000 routes.

Note To verify the number of statistics allocated or free on a line card, use the show mfib hardware resource-counters, on page 190 command in EXEC mode.

There are a limited number of counters on all nodes. When accounting on a prefix is enabled, counters are assigned to routes only if they are available.

To display packet statistics, use the **show mfib route** and the **show mfib hardware route statistics** commands. These commands display “N/A” for counters when no hardware statistics are available or when

neither the accounting per-prefix, on page 133 command nor the **accounting per-prefix forward-only** command are enabled.

You may switch between **accounting-perprefix** and **accounting per-prefix forward-only** statistics for ipv4 or ipv6 multicast family. However, be aware that only one set of counters is supported on the (*,G) routes (with fwd/punt/drop on ingress and fwd/drop on egress) regardless of whether you enabled the **accounting-perprefix** or **accounting-perprefix fwd-only** command.

Although you can switch accounting modes, this involves freeing the hardware statistics and reallocating them, thereby resulting in a loss of any previously collected data. Therefore, it is preferable to decide which statistics mode you want to use at the start to avoid the resource cost entailed by resetting the statistics counter values with a change in mode.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable accounting per-prefix forward-only for MVPN routing:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# accounting per-prefix forward-only
```

Related Commands

Command	Description
accounting per-prefix, on page 133	Enables accounting for multicast routing.
clear mfib hardware resource-counters, on page 145	Clears global resource counters.

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 2.0	This command was introduced.
Release 3.7.0	This command was documented as a multicast command.

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 172 command 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 159 command 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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#

RP/0/RP0/CPU0:router(config-mcast)# address-family ipv6
RP/0/RP0/CPU0:router(config-mcast-default-ipv6)#
```

This example shows how to enter IPv4 and IPv6 VRF multicast routing configuration submode:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# vrf vrf-name address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-vrf-name-ipv4)#

RP/0/RP0/CPU0:router(config-mcast)# vrf vrf-name address-family ipv6
RP/0/RP0/CPU0:router(config-mcast-vrf-name-ipv6)#
```

-

Related Commands

Command	Description
alias	Creates a command alias.
interface all enable, on page 157	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 159	Separates the disabling of multicast routing and forwarding.
interface (multicast), on page 155	Configures multicast interface properties.

boundary

To configure the multicast boundary on an interface for administratively scoped multicast addresses, use the **boundary** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

boundary *access-list*

no boundary *access-list*

Syntax Description

access-list	Access list specifying scoped multicast groups. The name cannot contain a space or quotation mark; it may contain numbers.

Command Default

A multicast boundary is not configured.

Command Modes

Multicast routing interface configuration

Multicast routing VRF interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	This command was supported in multicast routing VRF interface configuration mode.

Usage Guidelines

The **boundary** command is used to set up a boundary to keep multicast packets from being forwarded.

The boundary acl can specify a mcast source address in addition to a mcast group address. The keyword "any" can be added before the mcast group range.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set up a boundary for all administratively scoped addresses:

```
RP/0/RP0/CPU0:router(config) # ipv4 access-list myboundary2
RP/0/RP0/CPU0:router (config) # 10 deny ipv4 any 239.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(config) # 20 permit ipv4 any 224.0.0.0 15.255.255.255
RP/0/RP0/CPU0:router(config)# multicast-routing
```

```
RP/0/RP0/CPU0:router (config-mcast) # address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface GigE 0/2/0/2

RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# boundary myboundary2
```

clear mfib counter

To clear Multicast Forwarding Information Base (MFIB) route packet counters, use the **clear mfib counter** command in the appropriate mode.

clear mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **counter** [*group-address*| *source-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.
ipv6	(Optional) 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 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelin

Note This command only clears MFIB route packet software counters. To clear MFIB hardware statistics counters use the **clear mfib hardware route statistics** command.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to clear MFIB route packet counters on all nodes:

```
RP/0/RP0/CPU0: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** [**location** {*node-id*| **all**}]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
location *node-id*	(Optional) Clears global resource counters from the designated node.
all	The **all** keyword clears all global resource counters.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **location** keyword was changed from optional to required.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write, execute

Examples

The following example shows how to clear the Multicast Forwarding Information Base (MFIB) database on all nodes:

```
RP/0/RP0/CPU0:router# clear mfib database location all
```

clear mfib hardware resource-counters

To clear global resource counters, use the **clear mfib hardware resource-counters** command in EXEC mode.

clear mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware resource-counters** [**location** {*node-id*| **all**}]

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) Clears global resource counters from the designated node.
all	The **all** keyword clears all global resource counters.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added. The **location** keyword was changed from optional to required.
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **clear mfib hardware resource-counters** to estimate resource usage for an operation.

Task ID

Task ID	Operations
multicast	read, write, execute

Examples

The following example shows how to clear all global resource counters:

```
RP/0/RP0/CPU0:router# clear mfib hardware resource-counters location all
```

Related Commands

Command	Description
show mfib hardware resource-counters, on page 190	Displays the allocated and freed hardware resources for the Multicast Forwarding Information Base (MFIB) process.
show mfib hardware route statistics, on page 200	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.

clear mfib hardware route statistics

To reset all allocated counter values regardless of the Multicast Forwarding Information Base (MFIB) hardware statistics mode (accounting per-prefix or accounting per-prefix forward-only), use the clear mfib hardware route statistics command in EXEC mode.

clear mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware route statistics** {**egress**| **ingress**| **ingress-and-egress**} [*****| *source-address*] [*group-address* [*/prefix-length*]] [**location** {*node-id*| **all**}]

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.
egress	(Optional) Clears hardware statistics only on the specified outgoing route.
ingress	(Optional) Clears hardware statistics only on the specified incoming route.
ingress-and-egress	(Optional) Clears hardware statistics on both the incoming (ingress) and outgoing (egress) routes.
*****	(Optional) Clears shared tree route statistics.
source-address	(Optional) IP address or hostname of the multicast route source.
group-address	(Optional) IP address or hostname of the multicast group.
/ prefix-length	(Optional) 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). A slash must precede the decimal value.
location	(Optional) Clears route packet counters from the designated node.
node-id	The *node-id* argument is entered in the *rack/slot/module* notation.
all	The **all** keyword clears route packet counters on all nodes

Command Default

If not specified, IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added. The **location** keyword was changed from optional to required.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The Multicast Forwarding (MFWD) process exists on each line card and assigns hardware counters to each (S, G) route. Additionally, one global counter is assigned for all (*, G) routes, depending on resource availability.

To clear the set of counters for (*, G) routes, the MFWD process assigns a single set of counters to count packets that match (*, G) routes. Consequently, the **clear mfib hardware route statistics** command must be used in a form that either clears counters on all routes or matches all (*, G) routes.

Note This command only clears MFIB hardware statistics counters. To clear MFIB route packet software counters, use the **clear mfib counter** command.

This command can be used regardless of the statistics mode, in other words, either accounting per-prefix, on page 133 or accounting per-prefix forward-only, on page 135.

Note This command does not clear global (*, G) counters.

Task ID

Task ID	Operations
multicast	read, write, execute

Examples

The following command shows how to clear counters by route statistics for all multicast routes on both ingress and egress forwarding engines for the line card 0/1/CPU0:

```
RP/0/RP0/CPU0:router# clear mfib ipv4 hardware route statistics ingress-and-egress location
 0/1/CPU0
```

The following example shows how to clear the counters only on the ingress forwarding engine for (S, G) routes with the group address 224.1.1.1:

```
RP/0/RP0/CPU0:router# clear mfib hardware route statistics ingress 224.1.1.1 location
0/1/CPU0
```

Related Commands

Command	Description
accounting per-prefix, on page 133	Enables accounting for multicast routing.
accounting per-prefix forward-only, on page 135	Reduces hardware statistics resource allocations when enabling accounting, particularly for multicast VPN (MVPN).
show mfib hardware route statistics, on page 200	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.

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 2.0	This command was introduced.
Release 3.5.0	This command was supported in multicast routing VRF interface configuration mode.

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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# interface all enable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface GigE 0/1/0/0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

Related Commands

Command	Description
enable (multicast), on page 152	Enables multicast routing and forwarding on an interface.
interface all enable, on page 157	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 2.0	This command was introduced.
Release 3.5.0	This command was supported in multicast routing VRF interface configuration mode.

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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# interface GigE 0/1/0/0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# enable
```

Related Commands

Command	Description
disable (multicast), on page 150	Disables multicast routing and forwarding on an interface.
interface all enable, on page 157	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 3.8.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router# forwarding-latency delay 120
```

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 IPv6 multicast routing configuration

Multicast VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# interface all enable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# interface GigE 0/1/0/0

RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

Related Commands

Command	Description
disable (multicast), on page 150	Disables multicast routing and forwarding on an interface.
enable (multicast), on page 152	Enables multicast routing and forwarding on an interface.
interface all enable, on page 157	Enables multicast routing and forwarding on all new and existing interfaces.

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 2.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# interface all enable
RP/0/RP0/CPU0:router(config-mcast)# interface GigE 0/1/0/0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

Related Commands

Command	Description
disable (multicast), on page 150	Disables multicast routing and forwarding on an interface.
enable (multicast), on page 152	Enables multicast routing and forwarding on an interface.

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 or IPv6 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 or IPv6 configuration

Command History

Release	Modification
Release 3.5.0	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 or IPv6 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. Whereas, if used from the address-family ipv6 confguration submode, it prevents MLD and PIM IPv6 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/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface-inheritance disable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface loopback 1 enable

RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# show run router pim
```

With the **interface-inheritance disable** command in use, IGMP, or MLD, 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/RP0/CPU0:router(config-mcast-default-ipv4)# show run router igmp

router igmp
 vrf default
  interface GigabitEthernet0/6/0/3
   router enable
```

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 and IPv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable logging of trap events:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(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 and IPv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

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/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# maximum disable
```

mdt data

To configure multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN), use the **mdt data** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

mdt data *mdt-group-address*/*mask* [**threshold** *threshold-value*] [*acl-name*]

no mdt data *mdt-group-address*/*prefix-length* [**threshold** *threshold-value*] [*acl-name*]

Syntax Description

mdt-group-address	IP address of the MDT group.
/ *mask*	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.
threshold *threshold*	Specifies the traffic rate threshold to trigger data MDT. Range is 1 to 4294967295.
acl-name	Access list (ACL) for the customer's VRF groups allowed to perform data MDT.

Command Default

threshold : 1

Command Modes

Multicast routing configuration

Multicast routing address family IPv4 and IPv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.7.0	Additional keyword information was added to the command. The bottom of the threshold value range was increased by 1.

Usage Guidelines

When certain multicast streams exceed a configured bandwidth, the multicast data is moved to an MDT data group that is dynamically chosen from an available pool of multicast addresses. If the traffic bandwidth falls below the threshold, the source is switched back to the default MDT. To avoid transitions between the MDTs, traffic only reverts to the default MDT if traffic below the data MDT threshold is at least one minute old.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the data MDT group:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# mdt data 172.23.2.2/24 threshold 1200 acl_A
```

The following example shows how to configure the data MDT group from the multicast VRF submode:

```
RP/0/RP0/CPU0:router(config)# multicast-mcast)# maximum disablerouting
RP/0/RP0/CPU0:router(config-mcast)# vrf vrf-name mdt data 172.23.2.2/24
```

Related Commands

Command	Description
mdt default, on page 166	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).
mdt mtu, on page 168	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).
mdt source, on page 170	Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.

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* | **threshold** *value*]

no mdt data ingress replication[*acl_name* |**immediate-switch** | **number***value* | **threshold** *value*]

Syntax Description

immediate-switch	Enables switching to data MDT immediately.
acl_name	ACL fo vrf groups that are enabled for data MDT
number *value*	Maximum number of data MDTs to be triggered. Range is 1 to 262143.
immediate-switch *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 5.1.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to run the **mdt data ingress replication** command:

```
RP/0/RP0/CPU0:router (config-mcast-v1-ipv4) # mdt data ingress-replication immediate-switch
```

mdt default

To configure the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT), use the **mdt default** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

mdt default {*mdt-default-group-address*| **ipv4** *mdt-default-address*}

no mdt default {*mdt-default-group-address*| **ipv4** *mdt-default-address*}

Syntax Description

mdt-default-group-address	IP address of the MDT default group entered in *A.B.C.D.* format.
ipv4	Specifies IPv4-encapsulated MDT.
mdt-default-address	MDT IPv4 default address entered in *A.B.C.D.* format

Command Default

The MDT default group address must be unique.

Command Modes

Multicast routing configuration

Multicast routing address family IPv4 and IPv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.7.0	Additional keyword information was added.

Usage Guidelines

The default MDT has a unique group address used to create MVPN multicast tunnel interfaces.

Although within the multicast VRF configuration submode, the MDT configuration uses either the **ipv4** or **ipv6** keyword to distinguish the appropriate multicast VPN, the MDT core tree is IPv4.

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:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# mdt default
172.16.10.1
```

The following example shows how to configure the MDT default group address from multicast VRF configuration submode for an IPv6 address family:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# vrf vrf-name address-family ipv6
RP/0/RP0/CPU0:router(config-mcast-vrf-name-ipv6)#mdt default 172.16.10.1
```

Related Commands

Command	Description
mdt data, on page 163	Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).
mdt mtu, on page 168	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).
mdt source, on page 170	Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.

mdt mtu

To configure the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT), use the **mdt mtu** command in multicast VPN configuration mode. To remove this functionality, use the **no** form of this command.

mdt mtu *value*

no mdt mtu *value*

Syntax Description

value	Specifies the MTU value and ranges between 401 to 65535. The configured mdt mtu value includes 24 bytes of GRE encapsulation.

Command Default

The MDT tunnel default size is 1376.

Command Modes

Multicast VRF configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the MTU of the multicast distribution tree:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# vrf vrf_A
RP/0/RP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt mtu 2345
```

Related Commands

Command	Description
mdt data, on page 163	Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).
mdt default, on page 166	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).

Command	Description
mdt source, on page 170	Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.

mdt source

To configure the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address, use the **mdt source** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

mdt source *type interface-path-id*

no mdt source *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 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

Multicast routing address family IPv4 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.9.0	Per VRF MDT source feature was introduced.

Usage Guidelines

Use the **mdt source** command to identify the root of the multicast distribution tree in the service provider network. This address is used to update all MVPN peers through multiprotocol BGP.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the interface used to set the MDT source address:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# mdt source POS 0/1/0/0
```

Note Per VRF MDT Source is a new feature introduced in IOS XR Software Release 3.9.0 apart from the existing default MDT source. Each VRF can have its own MDT source interface co-existing with the default MDT source to achieve core diversity.

The following example shows how to configure a per VRF MDT source:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# mdt source loopback0
RP/0/RP0/CPU0:router(config-mcast)# vrf foo
RP/0/RP0/CPU0:router(config-mcast-foo)# address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-foo-ipv4)# mdt source loopback1 !
```

Related Commands

Command	Description
mdt data, on page 163	Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).
mdt default, on page 166	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).
mdt mtu, on page 168	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).

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 2.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enter multicast routing configuration mode:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)#
```

Related Commands

Command	Description
accounting per-prefix, on page 133	Enables per-prefix counters only in hardware.
alias	Creates a command alias.
interface (multicast), on page 155	Configures multicast interface properties.

Command	Description
interface all enable, on page 157	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**}]

[**address-family ipv6**] **multipath** [**hash** {**interface-extended**| **source next-hop**}]

no multipath

Syntax Description

hash	(Optional) Enables multipath hashing.
interface-extended	(Optional) Enables extensions for non-unique next-hop addresses. **Note** This option is available for IPv6 addressing in IPv6 multicast routing configuration mode and IPv6 multicast VRF configuration mode only.
source	Enables source-based multipath hashing.
source-nexthop	(Optional) Enables source with next-hop hashing.
source-specific-hash	(Optional) Enables multipath hashing for the source only. **Note** This option is available only for IPv6 addressing.

Command Default

This command is disabled by default.

Command Modes

Multicast routing configuration

Multicast routing address-family ipv4 and ipv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# 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 and ipv6 configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The **enable** and **disable** keywords.
Release 3.5.0	The **lifetime** *lifetime* keyword and argument were added.

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/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# nsf
```

Related Commands

Command	Description
nsf lifetime (IGMP/MLD)	Configures the maximum time for the NSF timeout value under IGMP or MLD.
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 233	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 3.2	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/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(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 and ipv6 configuration

Multicast VRF configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to enable individual route calculations:

```
RP/0/RP0/CPU0:router# multicast-routing vrf vpn12 address-family ipv4
RP/0/RP0/CPU0:router(config-mcast)# rate-per-route
```

Related Commands

Command	Description
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

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 3.4.0	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/RP0/CPU0:router# 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 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

show mfib counter

To display Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped, use the **show mfib counter** command in the appropriate 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.
ipv6	(Optional) Specifies IPv6 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

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 14: 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.
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 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mfib route, on page 214	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 3.5.0	This command was introduced.

Usage Guidelines

This feature is useful for Multicast VPN network implementations.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib encap-info** command:

```
RP/0/RP0/CPU0:router# 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 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

show mfib hardware interface

To display hardware switching interface information for the Multicast Forwarding Information Base (MFIB) process, use the **show mfib hardware interface** command in
EXEC mode

.

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware interface [detail]** [*type interface-path-id*] [**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.
detail	(Optional) Displays detailed information about the MFIB interface.
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.
location *node-id*	(Optional) Specifies an MFIB-designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.
Release 3.8.0	New fields were added to the output to show potential memory leakage or increased resource use.

Usage Guidelines

The **show mfib hardware interface** command displays multicast-specific information about the software switching interfaces of the router hardware. This command will not display any useful output if only RSP is specified or if no location is specified.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib hardware interface** command. The first line displays information for the fabric interface (FI0/1/1) on the line card. The fabric interface is a special interface that represents the hardware connection to the fabric.

```
RP/0/RP0/CPU0:router# show mfib ipv4 hardware interface location 0/1/cpu0

LC Type: Trident
Interface Handle Ghandle RefCnt TTL uIDB E-uIDB Parent-I/F Enbld Comment
BP1 0x800d0 0x0 3 0 (Bundle, no local members) success
BP2 0x800f0 0x0 3 0 (Bundle, no local members) success
FI0/1/CPU0 0x1180020 0x0 2 0 0 Unknwn Unknown False success
Te0/1/0/0 0x1180040 0x118004 3 0 1 1 N/A True success
Te0/1/0/1 0x1180060 0x118006 2 0 3 3 N/A True success
```

This table describes the significant fields shown in the display.

Table 15: show mfib hardware interface Field Descriptions

Field	Description
Interface	MFIB interface name.
Handle	A 32-bit system-wide identifier of the MFIB interface.
Ghandle	Global interface handle. A 28-bit system-wide identifier of the interface derived from the 32-bit handle, but does not exist for all MFIB interfaces.
RefCnt	Number of times various data structures referred to this MFIB interface structure.
TTL	Multicast time-to-live threshold that was configured on this MFIB interface.
uIDB	MicroIDB. A unique identifier of the MFIB interface that exists on the line card.
E-uIDB	An identifier that is relevant only for virtual MFIB interfaces such as bundles and tunnels. For example, if an interface is a member of a bundle, the effective uIDB is that of the bundle.

Field	Description
Parent-I/F	Parent interface handle. Relevant only for bundles and tunnels showing the corresponding parent MFIB interface handle.
Enbld	If true, multicast is enabled on the MFIB interface.
Primary IP	Primary IP address of the MFIB interface.
Secondary IP	Secondary IP address of the MFIB interface.
Bound-ACL	The following states appear for this field: • True if the multicast boundary is configured on the MFIB interface. • False if no boundary is configured. • Unknown if the MFIB interface is not applicable to multicast boundaries.
ADJ ADDR	Table lookup unit (TLU) memory location of the MFIB interface adjacency information.
Comment	Indicates whether there were problems when reading hardware information.

Related Commands

Command	Description
show mfib interface, on page 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.

show mfib hardware resource-counters

To display the allocated and freed hardware resources for the Multicast Forwarding Information Base (MFIB) process, use the **show mfib hardware resource-counters** command in EXEC mode .

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware resource-counters 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*	Specifies an MFIB-designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show mfib hardware resource-counters** command to understand the table lookup unit (TLU) resource usage by MFIB. The output shows the following:

- Usage for each channel
- Storing of specific data
- Allocation counts for metro statistics
- Failure counts for metro statistics

Note Use the location option in the **show mfib hardware resource-counters** command to indicate for which linecard you need information. The command will not display any useful output if only RSP is specified or if no location is specified.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib hardware resource-counters** command:

```
RP/0/RP0/CPU0:router# show mfib ipv4 hardware resource-counters location 0/1/cpu0

LC Type: Trident
TLU blocks channel 0 : ingress: 0,0      egress: 1,0
TLU blocks channel 1 : ingress: 0,0      egress: 0,0
TLU blocks channel 2 : ingress: 80329,80283      egress: 48041,48007
TLU blocks channel 3 : ingress: 202582,202576    egress: 48042,48007
TLU blocks for PLU_EXTENSION: 80329,80283
TLU blocks for S_BITMAP: 202582,202576
TLU blocks for USE_ACCEPT_BITMAP: 0,0
TLU blocks for CONN_CHECK: 0,0
TLU blocks for OLIST: 96083,96014
TLU blocks for L2_LOAD_INFO: 1,0
TLU blocks for L2_TE: 0,0
TLU blocks for OLIST1: 0,0
TLU blocks for OLIST2: 0,0
TLU blocks for ING_VPN_IPV4_ENCAP: 0,0
TLU blocks for EG_ACCEPT_BITMAP: 0,0
TLU blocks for P2MP_ENCAP: 0,0
TLU blocks for UNKNOWN: 0,0
Number of times having TLU block(s) allocation failures: 0
Number of times having TLU block(s) free failures: 0
Mstat success #calls: ingress: 3,0       egress: 2,0
Mstat failure #calls: ingress: 0,0       egress: 0,0

-- Shared Memory counters:
[table_ext] Alloc:      1 [          20 bytes]  Free:      0 [           0 byte]
[route_ext] Alloc:  80329 [    29882388 bytes]  Free:  80283 [    29865276 byte]
[intf_ext]  Alloc: 857102 [    47997712 bytes]  Free: 856905 [    47986680 byte]
[idb_ext]   Alloc:     27 [        2916 bytes]  Free:      7 [         756 byte]
[Encap_Info]Alloc:      0 [           0 bytes]  Free:      0 [           0 byte]
[TLU_Handle]Alloc: 277704 [    15551424 bytes]  Free: 277585 [    15544760 byte]
```

This table describes the significant fields shown in the display.

Table 16: show mfib hardware resource counters Field Descriptions

Field	Description
TLU blocks channel *n* : ingress: *n* egress: *n*	TLU blocks allocated on ingress and egress for each channel.
TLU blocks for PLU_EXTENSION	Resource use for storing extended data (in addition to the PLU lookup result).
TLU blocks for S_BITMAP	Resource use for storing a bitmap to indicate which interfaces have signaling turned on for this route.
TLU blocks for USE_ACCEPT_BITMAP	Resource use for bidirectional routes to indicate which interfaces can accept packets for this route.

Field	Description
TLU blocks for CONN_CHECK	Resource use for data type CONN_CHECK.
TLU blocks for OLIST	Resource use for data type OLIST.
TLU blocks for L2_LOAD_INFO	Resource use for data type L2_LOAD_INFO.

Related Commands

Command	Description
show mfib interface, on page 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.

show mfib hardware route accept-bitmap

To display platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes, use the **show mfib hardware route accept-bitmap** command in EXEC mode .

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware route accept-bitmap [*]** [*source-address*] [*group-address* [/*prefix-length*]] **[detail]** [**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.
*	(Optional) Displays shared tree entry.
source-address	(Optional) IP address or hostname of the multicast route source:
group-address	(Optional) IP address or hostname of the multicast group.
/ *prefix-length*	(Optional) 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). A slash must precede the decimal value.
detail	(Optional) Detailed list of the routing database.
location *node-id*	(Optional) Specifies an MFIB-designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelin

Note The command does not display any useful output if only RSP is specified or if no location is specified.

Task ID

Task ID	Operations
multicast	read

Examples

In the following example, the bidirectional range is configured as 233.1.0.0/16 and 233.4.0.0/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list bidir-range
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 233.1.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 233.4.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny any
RP/0/RP0/CPU0:router(config-ipv4-acl)# commit
RP/0/RP0/CPU0:router(config-ipv4-acl)# exit

RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# no rp-address 10.1.1.1 bidir
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# commit
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rp-address 10.1.1.1 bidir-range bidir
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# commit
```

The sample output from the **show mfib hardware route accept-bitmap** command displays the accepting interface list for (*,233.1.0.0/16) and (*,233.4.0.0/16) only. The accepting interface list is POS0/1/1/0, POS0/1/1/1, and POS0/1/1/3.

```
RP/0/RP0/CPU0:router# show mfib hardware route accept-bitmap detail location 0/1/CPU0

LC Type: Trident
Source: Source address                  Group: Group Address    M: Mask Length
iQoS  : Ingress QoS tag                 C    : Directly connected check flag
RPF   : Accepting interface for non-bidir entries
S     : Signal on RPF interface         FU   : For us
PLUext: PLU result extension address
FGID  : Fabric Group ID
oQoS  : Output QoS tag
FGID2 : Secondary Fabric Group ID
A_num    : Number of I/Fs in the accepting list
A_TLU    : Address of the first TLU in the accepting list
Interface: Accepting interface name
Source Group    M  iQoS C RPF  S FU PLUext  FGID  FGID2 P PF BA oQoS A_num A_TLU Interface
*   224.0.0.0   4  0    T Null F F  200ae2c 41785 -1    F F  T   0    0    Null
*   224.0.0.0   24 0    F Null F F  200d00f 47206 -1    F F  T   0    0    Null
*   224.0.1.39  32 0    F Null F F  200d000 47205 -1    T F  F   0    0    Null
*   224.0.1.40  32 0    F Null F F  200d00d 27202 -1    T F  F   0    0    Null
*   232.0.0.0   8  0    F Null F F  200d010 47207 -1    F F  T   0    0    Null
*   233.1.0.0   16 0    F Null F F  200ae34 44106 -1    F F  T   0    3    4400  PO0/1/1/0
*   233.1.0.0   16 0    F Null F F  200ae34 44106 -1    F F  T   0    3    4400  PO0/1/1/1
*   233.1.0.0   16 0    F Null F F  200ae34 44106 -1    F F  T   0    3    4400  PO0/1/1/3
*   233.1.1.1   32 0    F Null F F  200a418 27205 -1    F F  T   0    0    4400
*   233.1.1.2   32 0    F Null F F  200a419 27206 -1    F F  T   0    0    4400
*   233.1.1.3   32 0    F Null F F  200a41c 27207 -1    F F  T   0    0    4400
*   233.1.1.4   32 0    F Null F F  200a41d 27208 -1    F F  T   0    0    4400
*   233.4.0.0   16 0    F Null F F  200ae3c 42043 -1    F F  T   0    3    4500  PO0/1/1/0

*  233.4.0.0    16 0    F Null F F  200ae3c 42043 -1    F F  T   0    3    4500  PO0/1/1/3
```

```
RP/0/RP0/CPU0:router# show mfib hardware route accept-bitmap detail location 0/0/CPU0

LC Type: Trident
Source: Source address   Group: Group Address    M: Mask Length
        iQoS  : Ingress QoS tag                  C    : Directly connected check flag
        RPF   : Accepting interface for non-bidir entries
        S     : Signal on RPF interface          FU   : For us
        FGID  : Fabric Group ID
        oQoS  : Output QoS tag
        FGID2 : Secondary Fabric Group ID
        A_num    : Number of I/Fs in the accepting list
Interface: Accepting interface name
Source          Group           M
Source: *               Group: 224.0.0.0       Mask length: 24
Source: *               Group: 224.0.1.39      Mask length: 32
Source: *               Group: 224.0.1.40      Mask length: 32
Source: *               Group: 227.0.0.1       Mask length: 32
Source: 4.0.0.2         Group: 227.0.0.1       Mask length: 64
Source: *               Group: 230.0.0.0       Mask length: 8
Source: *               Group: 232.0.0.0       Mask length: 8
```

This table describes the significant fields shown in the display.

Table 17: show mfib hardware route accept-bitmap Field Descriptions

Field	Description
iQoS	An identifier of a quality-of-service (QoS) policy. This field is currently unused.
C	Directly connected check flag. If “T” is displayed, hardware performs directly connected checks on the packet sources that match this route.
S	Signal on Reverse Path Forwarding (RPF) interface. If “T” is displayed, hardware punts the packet to the line card CPU to signal Protocol Independent Multicast (PIM) (by default) for all packets that match this route.
FU	For us. A packet is destined for this router. If “T” is displayed, at least one application is interested in packets on one or more interfaces that match this route.
P	Punt. If “T” is displayed, all packets that match the route punt to the line card CPU.
PF	Punt if forward. If “T” is displayed, when the ingress hardware sends a packet to the egress line cards across the fabric, it also punts a copy of the packet to the line card CPU.
BA	Boundary access list (ACL). If “T” is displayed, the hardware punts the packet to the line card CPU for software switching when the incoming interface has a boundary access list configured.

Field	Description
oQoS	Output QoS policy identifier. This field is currently unused.
A_num	Number of accepting interfaces for a bidirectional route.

Related Commands

Command	Description
show mfib interface, on page 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.

show mfib hardware route olist

To display platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware, use the **show mfib hardware route olist** command in the appropriate mode.

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware route olist** {**[*]**| [*source-address*] [*group-address* [/**prefix-length**]] **[detail]**} [**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.
*	(Optional) Displays shared tree entries.
source-address	(Optional) IP address or hostname of the multicast route source.
group-address	(Optional) IP address or hostname of the multicast group.
/ *prefix-length*	(Optional) 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). A slash must precede the decimal value.
detail	(Optional) Displays a detailed list of the routing database. Requires 140 columns.
location *node-id*	Specifies an MFIB-designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show mfib hardware route olist** command displays the output interface list (olist) for each route. The Multicast Forwarding (MFWD) process stores olist interfaces in a table lookup unit (TLU) block (in groups of three). As such, the command displays each route three times. The command does not display any useful output if only RSP is specified or if no location is specified.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib hardware route olist** command for line card 0/1/CPU0 (the output fields are described in the header):

```
RP/0/RP0/CPU0:router# show mfib hardware route olist location 0/1/CPU0

LC Type: Trident
Source: Source address
Group : Group Address
M     : Mask Length
C     : Directly connected check flag
RPF   : Accepting interface for non-bidir entries
S     : Signal if packet arrived on RPF interface
FU    : For us
FGID  : Fabric Group ID
P     : Route Punt
PF    : Punt to CPU if packet is forwarded to the fabric
BA    : Check if boundary ACL is configured on incoming interface
O_Null   : Olist is empty
Interface: Output interface name
IC       : Internal copy flag
OP       : Output Punt: Punt instead of forwarding out
Source          Group           M  C RPF        S FU FGID   P PF BA O_Null Interface IC OP
   *            224.0.0.0       4  T Null       F F  41785  F F  T  True
   *            224.0.0.0       24 F Null       F F  47206  F F  T  True
   *            224.0.1.39      32 F Null       F F  47205  T F  F  True
   *            224.0.1.40      32 F Null       F F  27202  T F  F  True
   *            232.0.0.0       8  F Null       F F  47207  F F  T  True
   *            233.1.0.0       16 F Null       F F  44106  F F  T  False NULL
   *            233.1.0.0       16 F Null       F F  44106  F F  T  False NULL
   *            233.1.0.0       16 F Null       F F  44106  F F  T  False PO0/1/1/0  F  F
   *            233.1.1.1       32 F Null       F F  27205  F F  T  False NULL
   *            233.1.1.1       32 F Null       F F  27205  F F  T  False PO0/1/1/1  F  F
   *            233.1.1.1       32 F Null       F F  27205  F F  T  False PO0/1/1/0  F  F
   *            233.1.1.2       32 F Null       F F  27206  F F  T  False NULL
   *            233.1.1.2       32 F Null       F F  27206  F F  T  False PO0/1/1/1  F  F
   *            233.1.1.2       32 F Null       F F  27206  F F  T  False PO0/1/1/0  F  F
```

Related Commands

Command	Description
show mfib hardware route accept-bitmap, on page 193	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.
show mfib hardware route statistics, on page 200	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.

Command	Description
show mfib hardware route summary, on page 203	Displays summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

show mfib hardware route statistics

To display platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route, use the **show mfib hardware route statistics** command in EXEC mode.

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware route statistics [detail] [*]** [*source-address*] [*group-address* [/*prefix-length*]] [**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.
*	(Optional) Displays shared tree entries.
source-address	(Optional) IP address or hostname of the multicast route source.
group-address	(Optional) IP address or hostname of the multicast group.
/ *prefix-length*	(Optional) 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). A slash must precede the decimal value.
detail	(Optional) Displays a detailed list of the routing database.
location *node-id*	(Optional) Specifies an MFIB-designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show mfib hardware route statistics** command to display the hardware packet and byte counter for a route. Route counters are kept for (S, G) routes only. A single set of counters is provided for all

(*, G) routes.

This command displays the hardware packet and bytes count on a per-route basis. Per-route hardware counters are kept for (S, G) routes only. However, counters are managed dynamically and allocated on a priority basis and may not be available for each (S, G) route. There is a single set of counters for all

(*, G) routes. For example, interface counters and access list counters have higher priority than route counters.

Note Route counters are local to each line card.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib hardware route statistics** command for line card 0/1/CPU0.

The first four lines indicate that a total of 2709724 packets representing 184261232 bytes matched all (*, G) routes and were punted to line card CPU for further processing.

The second four lines indicate that 753 packets matched the route (10.1.1.9, 233.1.1.2), were accepted for forwarding, and were sent into the fabric by the ingress forwarding engine. The lines indicate that 749 packets and 47936 bytes were received by the egress forwarding engine from the fabric, matched (10.1.1.9, 233.1.1.2), and were sent out of at least one interface from the output interface list.

The command does not display any useful output if only RSP is specified or if no location is specified

```
RP/0/RP0/CPU0:router# show mfib hardware route statistics location 0/1/CPU0

LC Type: Trident
(*,G) Counter: Ingress Counter = 0xe170  Egress Counter = 0x9110
Ingress: Forward = (0 , 0)                  Punt = (2709724 , 184261232)
         Drop    = (0 , 0)
Egress:  Forward = (0 , 0)                 Drop = (0 , 0)
(10.1.1.9,233.1.1.1/64)  Ingress Counter = 0xe173  Egress Counter = 0x9112
Ingress: Forward = (753 , 51204)                   Punt = (0 , 0)
         Drop    = (0 , 0)
Egress:  Forward = (749 , 47936)                   Drop = (0 , 0)
```

This table describes the significant fields shown in the display.

Table 18: show mfib hardware route statistics Field Descriptions

Field	Description
Ingress Counter	Unique identifier of the ingress counter.
Egress Counter	Unique identifier of the egress counter.
Forward	Number of forwarded packets and bytes.
Punt	Number of bytes punted from the line card CPU.

Field	Description
Drop	Number of dropped bytes.

Related Commands

Command	Description
show mfib hardware route accept-bitmap, on page 193	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.
show mfib hardware route olist, on page 197	Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.
show mfib hardware route summary, on page 203	Displays summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

show mfib hardware route summary

To display summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry, use the **show mfib hardware route summary** command in EXEC mode.

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **hardware route summary 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 an MFIB-designated node.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show mfib hardware summary** command to display hardware information for the route of the node.

The longest-prefix match route is displayed depending on the provided source and group addresses. The command does not display any useful output if only RSP is specified or if no location is specified.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib hardware route summary** command:

```
RP/0/RP0/CPU0:router# show mfib hardware route summary location 0/1/cpu0
```

```
LC Type: Trident
H/W IP Multicast Forwarding Information Base Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 10

RP/0/RSP0/CPU0:router# show mfib hardware route summary location 0/0/CPU0

LC Type: Trident
H/W IP Multicast Forwarding Information Base Summary
  No. of (*,G) routes = 6
  No. of (S,G) routes = 5
  No. of (S,G) MoFRR routes = 0,   Maximum supported MoFRR routes = 1024

RP/0/RSP0/CPU0:router# show mfib hardware route summary location 0/4/cPU0

LC Type: A9K-SIP-700
Hardware IP Multicast Forwarding Information Base Route Summary
Number of hardware (*, G) routes = 6
Number of hardware (S, G) routes = 1
Number of hardware route-interfaces = 4
Number of hardware Rx adjacencies = 7
Number of hardware Tx adjacencies = 3
Number of ref to decap adjacency  = 0
Mvpn master LC status             = False
```

This table describes the significant fields shown in the display.

Table 19: show mfib hardware route summary Field Descriptions

Field	Description
No. of (*,G) routes	Number of (*,G) routes installed in hardware.
No. of (S,G) routes	Number of (S,G) routes installed in hardware.
Maximum supported MoFRR routes	Maximum number of MoFRR routes supported in hardware.

Related Commands

Command	Description
show mfib hardware route accept-bitmap, on page 193	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.
show mfib hardware route olist, on page 197	Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.
show mfib hardware route statistics, on page 200	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).

show mfib hardware session-info

To display hardware abstraction layer (HAL) session information for the Multicast Forwarding Information Base (MFIB) process, use the **show mifb hardware session-info** command in EXEC mode

.

show mfib [**ipv4**| **ipv6**] **hardware session-info location** *node-id*

Syntax Description

location *node-id*	Specifies an MFIB-designated node.
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 3.7.0	This command was introduced.

Usage Guidelin

Note This command is to be used only on request from Cisco Technical Support for troubleshooting. The command does not display any useful output if only RSP is specified or if no location is specified.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib hardware session-info** command:

```
RP/0/RP0/CPU0:router# show mfib hardware session-info location 0/3/cpu0
```

```
LC Type: Trident
HAL Session Info:(0x5276de8c):
default key(0x5276dcb0): vmr_id 0x2860009c:0x2860009b
default punt key(0x0): vmr_id 0x0:0x0
default cluster(0x5276dd4c): tlu address 0x2060000:0x0
default punt cluster(0x0): tlu address 0x0:0x0
default replicord(0x5276dde8): tlu address 0x0:0xa0000
mlc table sram addr: 0x1c8000
```

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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show mfib interface** command displays counters for the number of packets and bytes that are handled by software switching. Counters for packets processed by hardware are displayed by the appropriate **show mfib hardware** command.

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:

```
RP/0/RP0/CPU0:router# show mfib interface GigE 0/2/0/2 location 0/2/CPU0

Interface : GigE0/2/0/2 (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:

```
RP/0/RP0/CPU0: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 : GigE0/2/0/2 [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 20: 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.

Field	Description
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.

Related Commands

Command	Description
show mfib hardware interface, on page 187	Displays hardware switching interface information for the Multicast Forwarding Information Base (MFIB) process.

show mfib mdt statistics

To display information about mdt interface activity, use the **show mfib mdt statistics** command in EXEC mode.

show mfib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **mdt statistics**

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.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

```
RP/0/RP0/CPU0:router# show mfib vrf svpn1 mdt statistics

MDT Interface Statistics
      Input Pkts      Input Bytes  Output Pkts     Output Bytes
          591548        591540546            0                0
```

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**| **ipv6**] **nsf** [**location** *node-id*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 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 2.0	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/RP0/CPU0:router# 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 21: 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/MLD)	Configures the maximum time for the NSF timeout value under IGMP or MLD.
nsf (multicast) , on page 176	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.

Command	Description
show mrib nsf, on page 233	Displays the state of NSF operation in the MRIB.
show pim nsf	Displays the state of NSF operation for PIM.

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**| **ipv6**] **route** [**rate**| ***|** *source-IP-address*| *group-IP-address*/*prefix-length*| **detail**| **old-output**| **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* or *X:X::X.*
group-IP-address	(Optional) IP address or hostname of the multicast group. Format is: *A.B.C.D* or *X:X::X.*
/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* or *X:X::X/length* A slash must precede the decimal value.
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.
old-output	(Optional) Displays the old show output—available for backward compatibility.
rate	(Optional) Displays individual (S, G) rates.
sources-only	(Optional) Restricts display of any shared-tree entries.
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 2.0	This command was introduced.
Release 3.5.0	The **detail** keyword was added. The **vrf** *vrf-name* keyword and argument were added.

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. Counters for packets processed by hardware are displayed by the appropriate **show mfib hardware** command.

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.

The show mfib route rate command is not supported on interfaces such as bundle virtual interfaces and Bridge Group virtual interfaces (BVIs).

The command displays the rate per route for one line card in Multicast Forwarding Information Base (MFIB) table when the **statistics** keyword is used.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib route** command with the **location** keyword specified (the output fields are described in the header):

```
RP/0/RP0/CPU0:router# show mfib route location 0/1/CPU0
IP Multicast Forwarding Information Base Entry flags:
C - Directly-Connected Check, S - Signal, D - Drop,
  IA - Inherit Accept, IF - Inherit From, MA - MDT Address,
  ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
  MH - MDT interface handle, CD - Conditional Decap,
  DT - MDT Decap True
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  EG - Egress, EI - Encapsulation Interface, MI - MDT Interface SW/HW Forwarding Counts:
Packets in/Packets out/Bytes out SW Failure Counts: RPF / TTL / Empty Olist / Encap RL /
Other HW Drop Counts: Ingress / Egress HW Forwarding Rates: bps In/pps In/bps Out/pps Out
```

```
(*,224.0.0.0/4),   Flags:  C
  Last Used: 22:27:18
  SW Forwarding Counts: 608/0/0
  SW Failure Counts: 598/0/0/0
  HW Forwarding Counts: 840/6460964/284000578
  HW Drop Counts: N/A /N/A
  HW Forwarding Rates: N/A /N/A /N/A /N/A

(*,224.0.0.0/24),   Flags:  D
  Last Used: never
  SW Forwarding Counts: 0/0/0
  SW Failure Counts: 0/0/0/0
  HW Forwarding Counts: 0/6460964/284000578
  HW Drop Counts: N/A /N/A
  HW Forwarding Rates: N/A /N/A /N/A /N/A

.....
```

The following is sample output from the **show mfib route** command with the **summary** and **location** keywords specified:

```
RP/0/RP0/CPU0:router# show mfib route summary location 0/1/CPU0

IP Multicast Forwarding Information Base Summary
  No. of (*,G) routes = 20015
  No. of (S,G) routes = 20020
```

The following is sample output from the **show mfib route** command with the **statistics** and **location** keywords specified. For route *, 239.1.1.1, the hardware counters show N/A, which means no hardware statistic blocks were assigned to the route *, 239.1.1.1. However, routes 200.180.161.9 and 239.1.1.1 show that both hardware and software statistic blocks were assigned. The output fields are described in the header.

```
RP/0/RP0/CPU0:router# show mfib route statistics location 0/1/CPU0

IP Multicast Forwarding Information Base
Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,
  IA - Inherit Accept, IF - Inherit From, MA - MDT Address,
  ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
  MH - MDT interface handle, CD - Conditional Decap,
  DT - MDT Decap True
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  EG - Egress, EI - Encapsulation Interface, MI - MDT Interface
SW/HW Forwarding Counts: Packets in/Packets out/Bytes out
SW Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other
HW Drop Counts: Ingress / Egress
HW Forwarding Rates: bps In/pps In/bps Out/pps Out

(*,224.0.0.0/4), Flags: C
  Last Used: 03:24:50
  SW Forwarding Counts: 9038/0/0
  SW Failure Counts: 0/0/0/0
  HW Forwarding Counts: N/A /N/A /N/A
  HW Drop Counts: N/A /N/A
  HW Forwarding Rates: N/A /N/A /N/A /N/A

(*,224.0.0.0/24), Flags: D
  Last Used: never
  SW Forwarding Counts: 0/0/0
  SW Failure Counts: 0/0/0/0
  HW Forwarding Counts: N/A /N/A /N/A
  HW Drop Counts: N/A /N/A
  HW Forwarding Rates: N/A /N/A /N/A /N/A

(*,239.1.1.1), Flags: C
Last Used: 03:24:48
  SW Forwarding Counts: 3/0/0
  SW Failure Counts: 0/0/0/0
  HW Forwarding Counts: N/A /N/A /N/A
  HW Drop Counts: N/A /N/A
  HW Forwarding Rates: N/A /N/A /N/A /N/A
```

```
POS0/2/0/2 Flags: NS EG
POS0/2/0/1 Flags: NS EG

(200.180.161.9,239.1.1.1), Flags:
  Last Used: 00:01:08
  SW Forwarding Counts: 146/0/0
  SW Failure Counts: 0/0/0/0
  HW Forwarding Counts: 61327/61327/3924928
  HW Drop Counts: 0/0
  HW Forwarding Rates: N/A /N/A /N/A /N/A
POS0/2/0/2 Flags: NS EG
POS0/2/0/1 Flags: A EG

(*,239.1.1.2), Flags: C
  Last Used: 03:24:37
  SW Forwarding Counts: 7/0/0
  SW Failure Counts: 0/0/0/0
  HW Forwarding Counts: N/A /N/A /N/A
  HW Drop Counts: N/A /N/A
  HW Forwarding Rates: N/A /N/A /N/A /N/A
```

Related Commands

Command	Description
show mfib counter, on page 183	Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.
show mfib hardware route accept-bitmap, on page 193	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.
show mfib hardware route olist, on page 197	Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.
show mfib hardware route statistics, on page 200	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.
show mfib interface, on page 207	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
show mrib route, on page 235	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-id*| *vrf-name*} [**local**| **remote**] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Specifies IPv4 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 3.5.0	This command was introduced.
Release 3.6.0	The **local** and **remote** keywords were added.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mfib table-info** command showing the number of receiver VRF routes and the default MDT handle associated with this VRF in boldface.

```
RP/0/RP0/CPU0:router#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 22: 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.

Field	Description
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**| **ipv6**] **[old-output] 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.
old-output	(Optional) Displays the old show output—available for backward compatibility.
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 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

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/RP0/CPU0:router# 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 23: 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.

Field	Description
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.
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 211	Displays the state of a nonstop forwarding (NSF) operation for the Multicast Forwarding Information Base (MFIB) line cards.
show mfib route, on page 214	Displays route entries in the Multicast Forwarding Information Base (MFIB).
show mrib nsf, on page 233	Displays the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB).

show mrib fgid

To display the platform-specific Multicast Routing Information Base (MRIB) fabric group identifier (FGID) data, use the **show mrib fgid** command in EXEC mode .

show mrib fgid [**chkptdb**| **info**| **mstats**| **ostats**| **stats**| **nsf**]

Syntax Description

chkptdb	(Optional) Dumps the MRIB FGID checkpoint database.
info	(Optional) Displays the MRIB FGID information.
mstats	(Optional) Displays the MRIB FGID memory statistics.
ostats	(Optional) Displays the MRIB FGID operation statistics.
stats	(Optional) Displays the MRIB FGID statistics.
nsf	(Optional) Displays the NSF FGID statistics.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is the sample output from the **show mrib fgid chkptdb** command:

```
RP/0/RP0/CPU0:router# show mrib fgid chkptdb
Wed Sep 24 22:45:15.565 UTC

Number of FGIDs in the chkpt DB : 11000
All the chkpt entries with IP/Label ctx are dumped to a file /tmp/mrib_chkpt.txt in the
(D)RP.
```

```
To see the contents, run attach to the (D)RP
and copy to a tftp server: cp /tmp/mrib_chkpt.txt /tftp:<directory>' or print from the RP:
 'cat /tmp/mrib_chkpt.txt'
```

The following is the sample output from the **show mrib fgid info all** command:

```
RP/0/RP0/CPU0:router# show mrib fgid info all

Wed Sep 24 22:44:16.544 UTC

FGID information
----------------

FGID (type, TOS): 46080 (Primary, 9)
Context         : IP (0xe0000000, *, 224.0.1.39/32)
Members[ref]    : No LC associated with this FGID

FGID chkpt context valid : TRUE
FGID chkpt context :
                table_id 0xe0000000 group 0x270100e0/32 source 0x00000000
FGID chkpt info : 0x3000000
FGID chkpt fapid mask  :
                0x00000000 00000000 00000000 00000000 00000000
                  00000000 00000000 00000000 00000000
Joins batched  : 0
Leaves batched : 0
In PI retry list :N

FGID (type, TOS): 46081 (Primary, 9)
Context         : IP (0xe0000000, *, 224.0.1.40/32)
Members[ref]    : No LC associated with this FGID

FGID chkpt context valid : TRUE
FGID chkpt context :
                table_id 0xe0000000 group 0x280100e0/32 source 0x00000000
FGID chkpt info : 0x3000000
FGID chkpt fapid mask  :
                0x00000000 00000000 00000000 00000000 00000000
                  00000000 00000000 00000000 00000000
Joins batched  : 0
Leaves batched : 0
In PI retry list :N

FGID (type, TOS): 46082 (Primary, 9)
Context         : IP (0xe0000000, *, 224.0.0.0/24)
Members[ref]    : No LC associated with this FGID

FGID chkpt context valid : TRUE
FGID chkpt context :
                table_id 0xe0000000 group 0x000000e0/24 source 0x00000000
FGID chkpt info : 0x3000000
FGID chkpt fapid mask  :
                0x00000000 00000000 00000000 00000000 00000000
                  00000000 00000000 00000000 00000000
Joins batched  : 0
Leaves batched : 0
In PI retry list :N

FGID (type, TOS): 46083 (Primary, 9)
Context         : IP (0xe0000000, *, 232.0.0.0/8)
Members[ref]    : No LC associated with this FGID

FGID chkpt context valid : TRUE
FGID chkpt context :
                table_id 0xe0000000 group 0x000000e8/8 source 0x00000000
FGID chkpt info : 0x3000000
FGID chkpt fapid mask  :
                0x00000000 00000000 00000000 00000000 00000000
                  00000000 00000000 00000000 00000000
Joins batched  : 0
Leaves batched : 0
In PI retry list :N
```

The following is the sample output from the **show mrib fgid mstats** command:

```
RP/0/RP0/CPU0:router# show mrib fgid mstats

Wed Sep 24 22:44:31.749 UTC

FGID Memory statistics in Bytes
================================
iface_chunk_alloced       : 0
plat_chunk_alloced        : 116
join_chunk_alloced        : 176
fapnode_chunk_alloced      : 0
batch_chunk_alloced       : 0
batch_sid_chunk_alloced   : 0
lc_alloced                : 256
lmrib_plat_chunk_alloced  : 0
encapid_plat_chunk_alloced: 0
fgid_q_chunk_alloced      : 0
chkpt_q_chunk_alloced     : 0
fgid_pool_chunk_alloced   : 44176
```

The following is the sample output from the **show mrib fgid ostats** command:

```
RP/0/RP0/CPU0:router# show mrib fgid ostats
Wed Sep 24 22:44:38.244 UTC

MRIB PD operational stats from PI
=================================
Total FGID Request        : 4
Total FGID Release        : 0
Total FGID Req/Rel Failed : 0
Total FGID Joins          : 0
Total FGID Joins Failed   : 0
Total FGID UnJoins        : 0
Total FGID UnJoins Failed : 0

LMRIB PD operational stats from PI
==================================
Total FGID Request        : 0
Total FGID Release        : 0
Total FGID Req/Rel Failed : 0
Total FGID Joins          : 0
Total FGID Joins Failed   : 0
Total FGID UnJoins        : 0
Total FGID UnJoins Failed : 0

FGID Batch statistics
=====================
Current FGIDs Batched     : 0
Total Batch modify Joins  : 0
Total Batch modify Leaves : 0
FGID Joins Programmed     : 0
FGID Leaves Programmed    : 0

FGID Join/Leave Nullified : 0
FGID Sent & Not Nullified : 0

FGID Joins still in batch : 0
FGID Leaves still in batch: 0

FGID Aggregator statistics
==========================
Current Permit Bits               : 0x7

#Requests to FGID Alloc.          : 11
#Requests failed from FGID Alloc.  : 0

#Release to FGID Allocator         : 0
#Release failed from FGID Allocator: 0

Total # of JoinArray invoked      : 0
Total # of JoinArray retried      : 0
```

```
Total # of LeaveArray invoked      : 0
Total # of LeaveArray retried      : 0

FGID Aggr. Success Return          : 0
FGID Aggr. Flow Control            : 0
FGID Aggr. Error Return            : 0
FGID Aggr. Server Not Avail.       : 0

Total # of replays done from chkpt : 1
Total # of remarks done            : 1

FGID & Chkpt thread stats
=========================
Current FGID Q Depth            : 0
Max FGID Q Depth                : 0
Total FGID Thread Pulses        : 1

Current Chkpt Q Depth           : 0
Max Chkpt Q Depth               : 6000
Total Chkpt thread pulses       : 13
Total PI upds_done              : 13

MRIB init & FGID reuse time stamps
==================================
Platform init start time        : Sep 24 22:09:33.759
Platform init end time          : Sep 24 22:09:34.263
Checkpoint init start time      : Sep 24 22:09:34.174
Checkpoint init end time        : Sep 24 22:09:34.178
FGID replay start time          : Sep 24 22:09:34.291
FGID replay end time            : Sep 24 22:09:34.292
FGID reuse start time           : Sep 24 22:09:34.263
FGID reuse end time             : Jan  1 00:00:00.000
Stale(non-reuse) cleanup start  : Sep 24 22:12:36.316
Stale(non-reuse) cleanup end    : Sep 24 22:13:36.322

MRIB FGID Library Status  : MRIB_INIT MRIB_WAIT_FOR_FGID_PULSE MRIB_WAIT_FOR_CHKPT_PULSE
LMRIB_INIT
```

The following is the sample output from the **show mrib fgid stats** command:

```
RP/0/RP0/CPU0:router# show mrib fgid stats
Wed Sep 24 22:45:06.526 UTC

FGID FREE POOL STATISTICS
=========================
Total FGIDs from Allocator         : 11000
FGIDs Reused                       : 0
MRIB used FGIDs                    : 4
LMRIB used FGIDs                   : 0
ENCAPID used FGIDs                 : 0

Total FGIDs available              : 10996
Total FGIDs in USE                 : 4

FGID current pool head             : 4
FGID current pool tail             : 1000
FGID last pool head                : 0
FGID last pool tail                : 1000

FGID REUSE STATS
================
#FGIDs added to Joined-list        : 0
#FGIDs alloced from Joined-list    : 0
#FGIDs available in Joined-list    : 0

#IPs added to TRIE                 : 0
#IPs alloced from TRIE             : 0
#IPs available in TRIE             : 0

#LABELs added to TRIE              : 0
#LABELs alloced from TRIE          : 0
#LABELs available in TRIE          : 0
```

```
#ENCAP IDs added to TRIE           : 0
#ENCAP IDs alloced from TRIE       : 0
#ENCAP IDs available in TRIE       : 0

#Unused FGIDs freed                : 0
#Stale (non-reused) FGIDs freed    : 0

FGID CHECKPOINT STATS
=====================
FGID chunks create event to Q      : 11
#FGIDs chkpt created               : 11000
#FGIDs chkpt create failed         : 0

#FGIDs allocated to routes         : 4
#IP chkpt created                  : 4
#Label chkpt created               : 0
#ENCAP ID chkpt created            : 0
#FGID chkpt create failed          : 0
#IP chkpt create failed            : 0
#Label chkpt create failed         : 0
#ENCAP ID chkpt create failed      : 0

#FGIDs chkpt node-id mask saved    : 0
#FGIDs chkpt node-id mask failed   : 0

#FGIDs freed                       : 0
#IP freed                          : 0
#Label freed                       : 0
#ENCAP ID freed                    : 0

#FGIDs free failed                 : 0
#IP free failed                    : 0
#Label free failed                 : 0
#ENCAP ID free failed              : 0

#FGIDs delete event to Q           : 0
#FGIDs chkpt deleted               : 0
#FGIDs chkpt deleted failed        : 0

FGID REUSE CHECKPOINT STATS
===========================
#FGIDs read from chkptDB           : 0
#IPs read from chkptDB             : 0
#Labels read from chkptDB          : 0
#ENCAP IDs read from chkptDB       : 0

#FGIDs delete event to Q           : 0
#IP delete event to Q              : 0
#Label delete event to Q           : 0
#Encap ID delete event to Q        : 0

#FGIDs chkpt deleted               : 0
#IP chkpt deleted                  : 0
#Label chkpt deleted               : 0
#ENCAP ID chkpt deleted            : 0

#FGIDs chkpt deleted failed        : 0
#IP chkpt delete failed            : 0
#Label chkpt deleted failed        : 0
#ENCAP ID chkpt deleted failed     : 0

FGID LEAKS
==========
#Current FGIDs in FGID chkpt       : 11000
Total FGIDs from Allocator (reuse) : 11000
FGIDs Leak (create/read - delete)  : 0

#Current IPs in IP chkpt           : 4
FGIDs in Joined list (reuse)       : 4
IPs Leak (create/read - delete)    : 0

#Current Labels in Label chkpt     : 0
FGIDs in Joined list (reuse)       : 0
```

```
Labels Leak (create/read - delete) : 0

#Current Encap IDs in ENCAP chkpt  : 0
FGIDs in Joined list (reuse)       : 0
Encap IDs Leak (create/read - delete) : 0
```

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

```
RP/0/RP0/CPU0:router# show mrib fgid nsf
Wed Sep 24 22:44:48.966 UTC

NSF information
---------------
NSF state                 : INACTIVE
Currently in ISSU?        : NO
```

show mrib label-table-info

To display the Multicast Routing Information Base (MRIB) label table information, use the **show mrib label-table-info** command in EXEC mode .

show mrib label-table-info

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is the sample output from the **show mrib label-table-info** command:

```
RP/0/RP0/CPU0:router# show mrib label-table-info

VRF: default [tid 0xe0000000]
Registered Client:
  te_control [ccbid: 4 cltid: 778528 restart: 60000 recovery: 60000]
  lmrib_bcdl [ccbid: 2 cltid: 1 restart: 0 recovery: 0]
```

show mrib mdt-interface

To verify that the Multicast Routing Information Base (MRIB) has correctly learned multicast distribution tree (MDT) interface handles from Protocol Independent Multicast (PIM) and that it shows the corresponding table ID for each handle, use the **show mrib mdt-interface** command in EXEC mode.

show mrib mdt-interface [**detail**| **ifh**]

Syntax Description

detail	(Optional) Shows the dependent VRF routes for the MDT interface handles learned from PIM.
ifh	(Optional) Specifies the mapping for a particular MDT interface handle learned from PIM.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

You can use the **show mrib mdt-interface** command to help debug an MVPN route collapse in MRIB when Extranet VRF dependencies are introduced. For example, MRIB may learn about a route update from PIM with an MDT handle associated with a different VRF table than the source VRF table. This database can then be useful in verifying that the MDT handle for the dependent VRF has been learned correctly.

Task ID

Task ID	Operations
multicast	read

Examples

The following example illustrates detailed output from the **show mrib mdt-interface** command with the MDT interface handle name shown in parantheses in the output (mdtgreen):

```
RP/0/RP0/CPU0:router# show mrib mdt-interface detail

Fri Dec 12 00:12:16.001 UTC
IP Multicast MRIB MDT ifhandle Interface DB
MH - Handle update count, I - Intranet route count, EX - Extranet route count, Up - Uptime
```

```
0x9042b80(mdtvrf20)  TID:0xe0000014  MH:1  I:0  EX:0  Up:6d01h
    MDT route forward-reference DB:
0x9042c80(mdtvrf19)  TID:0xe0000013  MH:1  I:0  EX:0  Up:6d01h
    MDT route forward-reference DB:
0x9042d80(mdtvrf11)  TID:0xe000000b  MH:1  I:0  EX:0  Up:6d01h
    MDT route forward-reference DB:
0x9042e80(mdtvrf10)  TID:0xe000000a  MH:1  I:250  EX:0  Up:6d01h
    MDT route forward-reference DB:
    (18.18.10.2,232.0.0.1/32) [tid:0xe000000a] recollapse: FALSE
    (18.18.10.2,232.0.0.2/32) [tid:0xe000000a] recollapse: FALSE
    (18.18.10.2,232.0.0.3/32) [tid:0xe000000a] recollapse: FALSE
    (18.18.10.2,232.0.0.4/32) [tid:0xe000000a] recollapse: FALSE
...
```

This table describes the significant fields shown in the display.

Table 24: show mrib mdt-interface Field Descriptions

Field	Description
TID, tid	VRF table ID associated with the MDT handle.
MH	Number of times the MDT interface handle has been received. Used for debugging, because it allows you to identify duplicate updates. Under normal conditions, the value should be 1.
I	Number of intranet routes using a specific MDT interface handle.
EX	Number of extranet routes using a specific MDT interface handle.
Up	Uptime—Elapsed time since MDT interface handle was learned.
recollapse	Set to TRUE in situations where the MDT information (such as default MDT group or MDT interface handle) for a dependent VRF table was not received from PIM during a route collapse. The route will be “recollapsed” when all the dependent information is received.

When you use the **detail** keyword, the output displays dependent VRF routes. Otherwise, only the MDT interface mappings appear.

Related Commands

Command	Description
show mrib route-collapse, on page 239	Displays the contents of the Multicast Routing Information Base (MRIB) route-collapse database.

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**| **ipv6**] **[old-output] nsf**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
old-output	(Optional) Displays the old show output—available for backward compatibility.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	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/RP0/CPU0:router# 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 25: 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.
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 176	Configures the NSF capability for the multicast routing system.
nsf lifetime (IGMP/MLD)	Configures the maximum time for the NSF timeout value under IGMP or MLD.
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 route

To display all entries in the Multicast Routing Information Base (MRIB), use the **show mrib route** command in the appropriate mode .

show mrib [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **[old-output] route** [**summary**| **outgoing-interface**| [*****| *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.
ipv6	(Optional) Specifies IPv6 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. F ormat 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.*
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

EXEC

Command History

Release 2.0	This command was introduced.
Release 3.4.0	The **detail** keyword was added.

Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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 183 command displays global counters independent of the routes.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib route** command (the output fields are described in the header):

```
RP/0/RP0/CPU0:router# show mrib route

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
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface

(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
 Outgoing Interface List
  Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
 Outgoing Interface List
  POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
 Outgoing Interface List
  POS0/3/0/0 Flags: F NS LI
  Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
 Outgoing Interface List
  POS0/3/0/0 Flags: F NS
  Decapstunnel0 Flags: A
```

The following shows output when the **vrf** and **detail** keywords are used:

```
RP/0/RP0/CPU0:router# show mrib vrf vrf1 route detail
```

```
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
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet

(*,0.0.0.101) Ver: 0x818 Flags: MA, FMA: 0x0
  MDT Address: 5.5.5.5
  Up: 6d01h

(*,0.0.0.102) Ver: 0x5337 Flags: MA, FMA: 0x0
  MDT Address: 225.101.1.1
  Up: 6d01h

(*,0.0.0.103) Ver: 0x6cea Flags: ML, FMA: 0x0
  Master Linecard Slot: 0/3/CPU0
  Up: 6d01h

(*,0.0.0.104) Ver: 0x7ca Flags: MBH, FMA: 0x0
  BGP IFH:  0x9000180
  Up: 6d01h

(*,0.0.0.105) Ver: 0x5b67 Flags: MLF, FMA: 0x0
  Master Linecard Fallback Slot: 0/3/CPU0
  Up: 6d01h

(*,0.0.0.107) Ver: 0x382c Flags: MDT_IFH, FMA: 0x0
  Up: 6d01h
  MDT IFH:  0x9043d80
...
```

The following example shows detailed output for a source VRF route in a receiver on the source PE router in an MVPN extranet topology), with the MDT core tree ID of the receiver VRF displayed.

```
RP/0/RP0/CPU0:router# show mrib vrf vrf15 route 18.18.15.2 225.0.0.1 detail

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
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet
```

Related Commands

Command	Description
nsf lifetime (IGMP/MLD)	Configures the maximum time for the NSF timeout value on the IGMP.
show mfib counter, on page 183	Displays MFIB counter statistics for packets that have dropped.
show mrib route-collapse, on page 239	Displays the contents of the MRIB route collapse database.

Command	Description
show mrib mdt-interface, on page 231	Helps in troubleshooting whether or not MRIB has correctly learned the MDT interface handles from PIM, and whether or not the corresponding table ID for each handle is shown.
show mfib route, on page 214	Displays all entries in the MFIB table.

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**| **ipv6**] **route-collapse** [*core-tree*]

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.
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 3.5.0	This command was introduced.
Release 3.8.0	MVPN extanet attributes were added to the output for this command.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib route-collapse** command:

```
RP/0/RP0/CPU0:router# 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 235	Displays all entries in the Multicast Routing Information Base (MRIB).

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* or *X:X::X.*
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* or *X:X::X.*

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib route outgoing-interface** command:

```
RP/0/RP0/CPU0:router# 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 235	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**| **ipv6**] **table-info**

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.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.8.0	New MVPN extranet attributes were added to command output.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib table-info** command:

```
RP/0/RP0/CPU0:router# 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 26: 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.
MDT source	Per-VRF MDT source information.

Related Commands

Command	Description
show mrib tlc, on page 245	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**| **ipv6**] **tlc [remote]**

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.
remote	(Optional) Displays the linked remote entry.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	The **remote** keyword was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show mrib tlc** command:

```
RP/0/RP0/CPU0:router# 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 27: 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.

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 and 0 to 128 for IPv6.
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 2.0	This command was introduced.
Release 3.5.0	This command was supported in multicast VRF configuration mode.

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:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# vrf green
RP/0/RP0/CPU0:router(config-mcast)# static-rpf 10.0.0.1 32 GigE 0/0/5/0 10.1.1.1
```

Related Commands

Command	Description
show pim bsr candidate-rp	Displays PIM candidate rendezvous point information for the BSR.

ttl-threshold (multicast)

To configure the time-to-live (TTL) threshold for packets being forwarded out an interface, use the **ttl-threshold** command in the appropriate 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 : 0

Command Modes

Multicast routing interface configuration

Multicast routing VRF interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced as a replacement for the **multicast ttl-threshold** command.
Release 3.5.0	This command was supported in multicast routing VRF interface configuration mode.

Usage Guidelines

Only multicast packets with a TTL value greater than the threshold are forwarded out of the interface. The TTL threshold is compared to the TTL of the packet after it has been decremented by one and before being forwarded.

Configure the TTL threshold only on border routers.

Note Do not confuse this command with the **ttl-threshold (MSDP)** command in router MSDP configuration mode that is used to confine the multicast data packet TTL to be sent by an Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the TTL threshold to 23, which means that a multicast packet is dropped and not forwarded out of the GigE 0/1/0/0 interface:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# interface GigE 0/1/0/CPU0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# ttl-threshold 23
```

Related Commands

Command	Description
ttl-threshold (MSDP)	Limits which multicast data packets are sent in SA messages to an MSDP peer.

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**| **ipv6**]

no vrf *vrf-name* [**ipv4**| **ipv6**]

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.
ipv6	(Optional) Configures IPv6 address prefixes.

Command Default

No default behavior or values.

Command Modes

Multicast routing configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.7.0	ipv4 and ipv6 submodes were supported.

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/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# vrf vrf_1
RP/0/RP0/CPU0:router(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
boundary, on page 140	Configures a boundary to keep multicast packets from being forwarded.
accounting per-prefix, on page 133	Enables per-prefix counters only in hardware.
interface (multicast), on page 155	Configures multicast interface properties.
log-traps, on page 161	Enables logging of trap events.
mdt data, on page 163	Configures the MDT data group address range.
mdt default, on page 166	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).
mdt mtu, on page 168	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).
mdt source, on page 170	Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.
multipath, on page 174	Enables Protocol Independent Multicast (PIM) to divide the multicast load among several equal-cost paths.
rate-per-route, on page 180	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 247	Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.

Multicast PIM Commands

This chapter describes the commands used to configure and monitor Protocol Independent Multicast (PIM).

Note For PIM-related commands, IPv4 is the default IP address family; however, many commands, including **clear pim** and **show pim** , include both an IPv4 and IPv6 prefix. To run commands related to IPv6, you must use the IPv6 prefix. You do not need to specify the IPv4 prefix to run IPv4-related commands.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Cisco IOS XR Multicast Configuration Guide for the Cisco CRS Router*.

- accept-register, page 256
- auto-rp candidate-rp, page 257
- auto-rp listen disable, page 260
- auto-rp mapping-agent, page 261
- bsr-border, page 263
- bsr candidate-bsr, page 264
- bsr candidate-rp, page 266
- clear pim autorp, page 268
- clear pim bsr, page 270
- clear pim counters, page 272
- clear pim topology, page 275
- dr-priority, page 277
- embedded-rp , page 279
- global maximum, page 282
- global maximum bsr crp-cache threshold, page 284
- hello-interval (PIM), page 286
- interface (PIM), page 288

- interface all disable , page 290
- join-prune-interval, page 291
- join-prune-mtu, page 293
- maximum autorp mapping-agent-cache, page 294
- maximum group-mappings autorp, page 296
- maximum register-states, page 298
- maximum route-interfaces, page 299
- maximum routes, page 300
- mofrr, page 301
- neighbor-check-on-recv enable, page 304
- neighbor-check-on-send enable , page 305
- neighbor-filter, page 306
- nsf lifetime (PIM), page 307
- old-register-checksum, page 309
- router pim, page 311
- rp-address, page 313
- rpf topology route-policy, page 315
- rpf-redirect, page 317
- rpf-redirect bundle, page 318
- rpf-vector , page 320
- rp-static-deny , page 321
- show auto-rp candidate-rp, page 322
- show auto-rp mapping-agent, page 324
- show pim bgp-safi, page 326
- show pim bsr candidate-rp, page 328
- show pim bsr election, page 330
- show pim bsr rp-cache, page 332
- show pim context, page 334
- show pim context detail, page 337
- show pim context table, page 341
- show pim df election-state, page 343
- show pim df winner , page 346
- show pim global summary, page 348

- show pim group-map, page 350
- show pim interface, page 353
- show pim join-prune statistic, page 356
- show pim rpf-redirect, page 358
- show pim rpf-redirect route, page 360
- show pim mdt, page 361
- show pim mstatic, page 363
- show pim neighbor, page 365
- show pim nsf, page 368
- show pim range-list, page 370
- show pim rpf, page 372
- show pim rpf hash, page 374
- show pim rpf route-policy statistics, page 377
- show pim rpf route-policy test, page 379
- show pim rpf summary, page 381
- show pim summary, page 383
- show pim table-context, page 385
- show pim topology, page 387
- show pim topology detail, page 393
- show pim topology entry-flag, page 396
- show pim topology interface-flag, page 399
- show pim topology summary, page 402
- show pim traffic, page 404
- show pim tunnel info, page 407
- spt-threshold infinity, page 409
- ssm, page 410

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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# accept-register no-ssm-range
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RP0/CPU0:router(config)# ipv4 access-list no-ssm-range
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny ipv4 any 232.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(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 2.0	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.

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list 5
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 224.0.0.0 15.255.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# auto-rp candidate-rp GigE 0/1/0/1 scope 31
group-list 5
RP/0/RP0/CPU0: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:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list 10
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 239.254.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# auto-rp candidate-rp loopback 0 scope 16
group-list 10
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# end
```

Related Commands

Command	Description
auto-rp mapping-agent, on page 261	Configures the router to be a rendezvous point (RP) mapping agent on a specified interface.

auto-rp listen disable

To prevent a Protocol Independent Multicast (PIM) process from learning about IP multicast traffic for the auto-rendezvous point (Auto-RP) group 224.0.1.40 that is flooded across interfaces, use the **auto-rp listen disable** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

auto-rp listen disable

no auto-rp listen disable

Command Default

PIM rendezvous point mappings are learned through Auto-RP.

Command Modes

PIM configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelin

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

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to disable rendezvous point discovery:

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# auto-rp listen disable
```

auto-rp mapping-agent

To configure the router to be a rendezvous point (RP) mapping agent on a specified interface, use the **auto-rp mapping-agent** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

auto-rp mapping-agent *type interface-path-id* **scope** *ttl-value* [**interval** *seconds*]

no auto-rp mapping-agent

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 time-to-live (TTL) value in router hops that limits the scope of the rendezvous point discovery messages that are sent from that interface. Range is 1 to 255.
interval *seconds*	(Optional) Specifies the time, in seconds, between discovery messages. Range is 1 to 600.

Command Default

A router is not configured as a Protocol Independent Multicast (PIM) rendezvous point mapping agent by default.

seconds : 60

Command Modes

PIM configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

After the router is configured as a rendezvous point mapping agent and determines the rendezvous point-to-group mappings through the CISCO-RP-ANNOUNCE (224.0.1.39) group, the router sends the mappings in an auto-rendezvous point (Auto-RP) discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). A PIM designated router (DR) listens to this well-known group to determine which rendezvous point to use.

More than one rendezvous point mapping agent can be configured in a network sending redundant information, for a slight increase in reliability.

The TTL value is used to limit the range, or scope, of a multicast transmission. Therefore, use this value only on border routers.

The mapping packets are always sourced out of the default interface but have the source IP address as the address of the *type* and *instance* arguments. Packets have a TTL of 1 to 255 and are sent out each configured interval. When not specified, the default is 60 seconds.

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

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to limit Auto-RP discovery messages to 20 hops:

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# auto-rp mapping-agent pos 0/0/0/1 scope 20
```

Related Commands

Command	Description
auto-rp candidate-rp, on page 257	Configures 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).

bsr-border

To stop the forwarding of bootstrap router (BSR) messages on a Protocol Independent Multicast (PIM) router interface, use the **bsr-border** command in PIM interface configuration mode. To return to the default behavior, use the **no** form of this command.

bsr-border

no bsr-border

Command Default

BSR messages are forwarded on the PIM router interface.

Command Modes

PIM interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

When you configure the **bsr-border** command, no PIM Version 2 BSR messages are sent or received through the interface. You should configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Note This command is used for the purpose of setting up a PIM domain BSR message border, and not for multicast boundaries.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the Packet-over-SONET/SDH (POS) 0/1/0/0 interface to be the PIM domain border:

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# bsr-border
```

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 3.2	This command was introduced.
Release 4.3	PIM BSR limits were introduced for this command.

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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-bsr 10.0.0.1 hash-mask-len 30
```

Related Commands

Command	Description
clear pim bsr, on page 270	Clears bootstrap router (BSR) entries from the Protocol Independent Multicast (PIM) rendezvous point (RP) group mapping cache.
show pim bsr candidate-rp, on page 328	Displays Protocol Independent Multicast (PIM) candidate rendezvous point (RP) information for the bootstrap router (BSR).
show pim bsr election, on page 330	Displays Protocol Independent Multicast (PIM) candidate election information for the bootstrap router (BSR).

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*]

no bsr candidate-rp *ip-address*

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 3.2	This command was introduced.
Release 4.3	PIM BSR limits were introduced for this command.

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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-rp 172.16.0.0 group-list 4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RP0/CPU0:router(config)# ipv4 access-list 4
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 239.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# end
```

Related Commands

Command	Description
bsr candidate-bsr, on page 264	Configures the router to announce its candidacy as a bootstrap router (BSR).

clear pim autorp

To clear auto-rendezvous point (Auto-RP) entries from the Protocol Independent Multicast (PIM) rendezvous point (RP) group mapping cache, use the **clear pim autorp** command in EXEC mode.

clear pim [**vrf** *vrf-name*] **[ipv4] autorp** [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
rp-address	(Optional) Hostname or IP address of the rendezvous point, entered in *A.B.C.D.* format.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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 Auto-RP entries have been cleared from the PIM rendezvous point group mapping cache:

```
RP/0/RP0/CPU0:router# 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     static    1          0.0.0.0
224.0.1.40/32*  DM     static    1          0.0.0.0
224.0.0.0/24*   NO     static    0          0.0.0.0
232.0.0.0/8*    SSM    config    0          0.0.0.0
224.0.0.0/4*    SM     autorp    0          10.1.1.1   RPF: De0,10.1.1.1 (us)
224.0.0.0/4     SM     static    0          0.0.0.0    RPF: Null,0.0.0.0

RP/0/
RP0
```

```
/CPU0:router# clear pim autorp 232.0.0.0/8

RP/0/
RP0
```

```
/CPU0:router# 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     static    1          0.0.0.0
224.0.1.40/32*  DM     static    1          0.0.0.0
224.0.0.0/24*   NO     static    0          0.0.0.0
224.0.0.0/4*    SM     static    0          0.0.0.0    RPF: Null,0.0.0.0
```

clear pim bsr

To clear bootstrap router (BSR) entries from the Protocol Independent Multicast (PIM) rendezvous point (RP) group mapping cache, use the **clear pim bsr** command in EXEC mode.

clear pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **bsr**

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.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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 the BSR group mappings have been cleared from the rendezvous point group mapping cache:

```
RP/0/RP0/CPU0:router# 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    static 0      0.0.0.0
224.0.1.40/32*       DM    static 1      0.0.0.0
224.0.0.0/24*        NO    static 0      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    bsr+   1      91.1.1.1        RPF: De0,91.1.1.1 (us)
224.0.0.0/4          SM    static 0      0.0.0.0         RPF: Null,0.0.0.

RP/0/RP0/CPU0:router# clear pim bsr
RP/0/RP0/CPU0:router# 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    static 0      0.0.0.0
224.0.1.40/32*       DM    static 1      0.0.0.0
224.0.0.0/24*        NO    static 0      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    static 1      0.0.0.0         RPF: Null,0.0.0.0
```

Related Commands

Command	Description
show pim group-map, on page 350	Displays group-to-PIM mode mapping.

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**| **ipv6**] **counters**

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.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 28: 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.

Field	Description
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/RP0/CPU0:router# clear pim counters
RP/0/RP0/CPU0:router# 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 404	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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# dr-priority 2
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# dr-priority 4
```

embedded-rp

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

embedded-rp *rp-address access-list* **[disable]**

Syntax Description

rp-address	Rendezvous point IPv6 address in *X:X::X* format.
access-list	Number or name of an IPv6 address access list that specifies embedded group ranges.
disable	Disables embedded RP processing.

Command Default

The static address for the embedded rendezvous point is not configured by default.

Command Modes

PIM configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

When the embedded rendezvous point is enabled (which is the default behavior of the PIM router), you should configure a static address for the rendezvous point for the embedded rendezvous point ranges. Additional configuration is not required on other IPv6 PIM routers, because those routers discover the rendezvous point address from the IPv6 group address.

Note The **embedded-rp** command is available only for IPv6 address prefixes.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to configure the static address for the embedded rendezvous point and specify an access list for group ranges:

```
RP/0/RP0/CPU0:router(config)# router pim address-family ipv6
RP/0/RP0/CPU0:router(config-pim-ipv6)# embedded-rp 2:2:2::2 acl_embed
RP/0/RP0/CPU0:router(config)# ipv6 access-list acl_embed
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

The following sample output displays the embedded rendezvous point information that was previously configured:

```
RP/0/RP0/CPU0:routerrouter# show pim ipv6 group-map

IP PIM Group Mapping Table
(* indicates group mappings being used)
(+ indicates BSR group mappings active in MRIB)

Group Range                                             Proto Client   Groups

ff02::/16*                                              NO    perm     0
  RP: ::
ff12::/16*                                              NO    perm     0
  RP: ::
ff22::/16*                                              NO    perm     0
  RP: ::
ff32::/16*                                              NO    perm     0
  RP: ::
ff42::/16*                                              NO    perm     0
  RP: ::
.
.
.
ff73:240:2:2:2::/96*                                    SM    embd-cfg 0
  RP: 2:2:2::2
  RPF: De6tunnel0,2:2:2::2 (us)
ff74:240:2:2:2::/96*                                    SM    embd-cfg 0
  RP: 2:2:2::2
  RPF: De6tunnel0,2:2:2::2 (us)
ff75:240:2:2:2::/96*                                    SM    embd-cfg 0
  RP: 2:2:2::2
  RPF: De6tunnel0,2:2:2::2 (us)
ff76:240:2:2:2::/96*                                    SM    embd-cfg 0
  RP: 2:2:2::2
  RPF: De6tunnel0,2:2:2::2 (us)
ff77:240:2:2:2::/96*                                    SM    embd-cfg 0
  RP: 2:2:2::2
  RPF: De6tunnel0,2:2:2::2 (us)
ff78:240:2:2:2::/96*                                    SM    embd-cfg 0
  RP: 2:2:2::2
  RPF: De6tunnel0,2:2:2::2 (us)
ff70::/12*                                              SM    embd     0
  RP: ::
  RPF: Null,::
fff0::/12*                                              NO    embd     0
  RP: ::
ff33::/32*                                              SSM   config   0
  RP: ::
```

Related Commands

Command	Description
rp-address, on page 313	Statically configures the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group.
show pim group-map, on page 350	Displays group-to-PIM mode mapping.

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 3.9.0	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/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(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 4.2.0	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/RP0/CPU0:router# router pim

RP/0/RP0/CPU0:router(config-pim)# global maximum bsr crp-cache 2000 ?
   threshold  Set threshold to print warning
   <cr>
RP/0/RP0/CPU0:router(config-pim)# global maximum bsr crp-cache 2000 threshold ?
   <1-2000>  Threshold value
RP/0/RP0/CPU0:router(config-pim)# global maximum bsr crp-cache 2000 threshold 500
RP/0/RP0/CPU0:router(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/RP0/CPU0:router# router pim

RP/0/RP0/CPU0:router(config-pim)# address-family ipv4

RP/0/RP0/CPU0:router(config-pim-default-ipv4)# global maximum bsr crp-cache 2000 threshold
 500

RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum bsr crp-cache 1800 threshold 450

RP/0/RP0/CPU0:router(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/RP0/CPU0:router# router pim

RP/0/RP0/CPU0:router(config-pim)# address-family ipv4

RP/0/RP0/CPU0:router(config-pim-default-ipv4)# global maximum bsr crp-cache 600 threshold
550

RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum bsr crp-cache 500 threshold 450

RP/0/RP0/CPU0:router(config-pim-default-ipv4)#
```

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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# hello-interval 45
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# hello-interval 60
```

Related Commands

Command	Description
dr-priority, on page 277	Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.
show pim neighbor, on page 365	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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router
/CPU0:router(config-pim-ipv4-if)#
```

Related Commands

Command	Description
dr-priority, on page 277	Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.
hello-interval (PIM), on page 286	Configures the frequency of Protocol Independent Multicast (PIM) hello messages.
join-prune-interval, on page 291	Configures the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic.

interface all disable

To disable Protocol Independent Multicast (PIM) processing on all interfaces, use the **interface all disable** command in PIM configuration mode. To re-enable PIM processing on all interfaces, use the **no** form of this command.

interface all disable

no interface all disable

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to disable PIM processing on all interfaces:

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface all disable
```

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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(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 4.3.1	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

Examples

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

```
RP/0/RP0/CPU0:router (config-pim) # join-prune-mtu 1000
```

maximum autorp mapping-agent-cache

To configure the maximum cache setting for an auto-rendezvous point (Auto-RP), use the **maximum autorp mapping-agent-cache** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

maximum autorp mapping-agent-cache *cache-size*

no maximum autorp mapping-agent-cache

Syntax Description

cache-size	(Required) Specifies the mapping agent cache. Maximum cache size range is 1 to 100.

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the maximum mapping agent cache size to 66:

```
RP/0/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum autorp mapping-agent-cache 66
```

Related Commands

Command	Description
maximum group-mappings autorp, on page 296	Configures the maximum number of Protocol Independent Multicast (PIM) group map ranges learned through the auto-rendezvous point (Auto-RP) mechanism.

Command	Description
show pim summary, on page 383	Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.

maximum group-mappings autorp

To configure the maximum number of Protocol Independent Multicast (PIM) group map ranges learned through the auto-rendezvous point (Auto-RP) mechanism, use the **maximum group-mappings** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

maximum group-mappings autorp *number*

no maximum group-mappings autorp

Syntax Description

number	Maximum number of PIM group mappings. Range is 1 to 5000.

Command Default

number : 500

Command Modes

PIM configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	This command was introduced.

Usage Guidelines

The **maximum group-mappings autorp** command lets you set the upper limit for the PIM out-of-resource (OOR) configuration range. The range is initiated from the Auto-RP mapping agent announcement. When the limit has been reached, PIM does not create additional Auto-RP group mapping ranges.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows how to set the upper limit number for group mapping to 200:

```
RP/0/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum group-mappings autorp 200
```

Related Commands

Command	Description
maximum autorp mapping-agent-cache, on page 294	Configures the maximum cache setting for an auto-rendezvous point (Auto-RP).
show pim summary, on page 383	Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.

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 2.0	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/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum register-states 10000
```

Related Commands

Command	Description
show pim summary, on page 383	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 2.0	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/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum route-interfaces 200000
```

Related Commands

Command	Description
show pim summary, on page 383	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 2.0	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/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum routes 200000
```

Related Commands

Command	Description
show pim summary, on page 383	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/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 configuration mode.

mofrr rib *acl_name*

no rib *acl_name*

Syntax Description

acl_name	Specifies the flows (S, G) s to be enabled by MoFRR.
rib	Configures MoFRR based on RIB convergence.

Command Default

MoFRR is not enabled by default.

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

Command Modes

PIM configuration

PIM vrf configuration

PIM address-family IPv4 and IPv6 configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

MoFRR is a mechanism in which two copies of the same multicast stream flow through disjoint paths in the network. At the point in the network (usually the PE closer to the receivers) where the two streams merge, one of the streams is accepted and forwarded on the downstream links, while the other stream is discarded.
.

MoFRR is triggered when a failure is detected on the primary path. MoFRR transmits a multicast join message to PIM from a receiver towards a source on a primary path and then transmits a secondary multicast join message from the receiver towards the source on a backup path. Data packets are received from the primary and secondary paths, with the redundant packets being discarded at topology merge points based on reverse-path forwarding (RPF) checks.

Note Triggered joins are sent when the primary or the secondary RPF information changes. No RPF change prunes are sent for MoFRR streams.

When a failure is detected on the primary path, the repair occurs by changing the interface on which packets are accepted to the secondary interface. Because the repair is local, it is fast and greatly improves convergence times should link or node failures occur on the primary path.

MoFRR switchover occurs at the software level in PIM, based on RIB convergence. Convergence-based switchovers can occur at a frequency of approximately 200 ms for an estimated 400 streams.

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:

```
RP/0/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim)# mofrr rib acl-green

RP/0/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim)# address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# mofrr acl-green
```

Related Commands

Command	Description
show mfib counter	Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.
show mfib route	Displays route entries in the MFIB.
show mrib route	Displays all entries in the Multicast Routing Information Base (MRIB).
show pim rpf hash, on page 374	Displays MoFRR hashing information for Routing Information Base (RIB) lookups used to predict RPF next-hop paths for routing tables in PIM.
show pim rpf summary, on page 381	Displays summary information about the interaction of PIM with the RIB.
show pim topology detail, on page 393	Displays detailed PIM routing topology information that includes references to the tables in which reverse path forwarding (RPF) lookups occurred for specific topology route entries.

Command	Description
show pim topology, on page 387	Displays PIM routing topology table information for a specific group or all groups.

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 3.2	This command was introduced as **neighbor-check-on-recv disable** .
Release 3.4.0	Command was changed to **neighbor-check-on-recv enable** .

Usage Guidelines

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/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# neighbor-check-on-recv enable
```

Related Commands

Command	Description
neighbor-check-on-send enable , on page 305	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 3.2	This command was introduced as **neighbor-check-on-send disable** .
Release 3.4.0	Command was changed to **neighbor-check-on-send enable** .

Usage Guidelines

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/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# neighbor-check-on-send enable
```

Related Commands

Command	Description
neighbor-check-on-recv enable, on page 304	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 2.0	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/RP0/CPU0:router(config-pim-default-ipv4)# neighbor-filter 1
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RP0/CPU0:router(config)# ipv4 access-list 1
RP/0/RP0/CPU0:router(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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 30
```

Related Commands

Command	Description
nsf (multicast)	Turns on NSF capability for the multicast routing system.

Command	Description
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 368	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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(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 2.0	This command was introduced.
Release 3.2	The **address-family** keyword was added.

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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(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/RP0/CPU0:router(config)# router pim address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)#

RP/0/RP0/CPU0:router(config)# router pim address-family ipv6
RP/0/RP0/CPU0:router(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 2.0	This command was introduced.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) or bidir domain 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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(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/RP0/CPU0:router(config)# ipv4 access-list 1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 225.2.2.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-ipv4)# rp-address 172.16.6.21
RP/0/RP0/CPU0:router(config-pim-ipv4)#
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rp-address 172.16.6.21
```

The following example shows how to set the PIM rendezvous point address to 172.17.1.1 to serve the bidirectional group range defined in access list user1:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list user1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 230.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rp-address 172.17.1.1 user1 bidir
RP/0/RP0/CPU0:router(config-pim-default-ipv4)#
```

Related Commands

Command	Description
ipv4 access-list	Defines a standard IP access list. For more information, see *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router*

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 3.7.0	This command was introduced.

Usage Guidelines

For information about routing policy commands and how to create a routing policy, see *Cisco IOS XR Routing Command Reference for the Cisco CRS Router* and *Cisco IOS XR Routing Configuration Guide for the Cisco CRS Router*.

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 and IPv6 address family prefixes:

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rpf topology route-policy mypolicy
```

```
RP/0/RP0/CPU0:router(config)# router pim address-family ipv6
RP/0/RP0/CPU0:router(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 4.3.0	This command was introduced.

Usage Guidelines

For information about routing policy commands and how to create a routing policy, see *Cisco IOS XR Routing Command Reference for the Cisco CRS Router* and *Cisco IOS XR Routing Configuration Guide for the Cisco CRS Router*.

Task ID

Task ID	Operation
Multicast	read, write

Examples

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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim)#address-family ipv4
RP/0/RP0/CPU0:router(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 4.3.0	This command was introduced.

Usage Guidelines

For information about routing policy commands and how to create a routing policy, see *Cisco IOS XR Routing Command Reference for the Cisco CRS Router* and *Cisco IOS XR Routing Configuration Guide for the Cisco CRS Router*.

Task ID

Task ID	Operation
Multicast	read, write

Examples

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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim)#address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# hello-interval 1
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# join-prune-interval 15
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rpf-redirect route-policy directv
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 60
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface GigabitEthernet0/0/4/7
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# enable
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# rpf-redirect bundle WEST bandwidth 6000 threshold
 5000
```

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 3.3.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rpf-vector
```

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 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rp-static-deny listA
```

Related Commands

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

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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** keyword was added.

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/RP0/CPU0:router# 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 29: 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.
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.

Related Commands

Command	Description
auto-rp mapping-agent, on page 261	Configures the router to be a rendezvous point (RP) mapping agent on a specified interface.

show auto-rp mapping-agent

To display the mapping agent cache, use the **show auto-rp mapping-agent** command in EXEC mode .

show auto-rp [ipv4] mapping-agent

Syntax Description

ipv4	(Optional) Specifies a particular IPv4 address prefix.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **trace** keywords were added.

Usage Guidelines

The **show auto-rp mapping-agent** command shows all the system-wide candidate rendezvous point (RP) announcements that originate from the same or different multicast groups.

Information that is displayed shows that the mapping agent selects one rendezvous point for the group. If two rendezvous point announcements are bound for the same group, the mapping agent selects the one with the higher IP address as the “winner” and sends that out to the CISCO-RP-DISCOVERY group. All multicast routers join this group.

Task ID

Task ID	Operations
multicast	read

Examples

The following sample output shows that the mapping agent has received two candidate rendezvous point announcements for the same group range (224/4) and has selected the one with the higher IP address (winner indicated by a *):

```
RP/0/RP0/CPU0:router# show auto-rp mapping-agent

Mapping Agent Table
10.0.0.6 (expire : 80 secs)
  224.0.0.0/4  SM  *
```

```
10.0.0.2 (expire : 75 secs)
  224.0.0.0/4   SM
```

This table describes the significant fields shown in the display.

Table 30: show auto-rp mapping-agent Field Descriptions

Field	Description
10.0.0.6	Rendezvous point address of the advertised candidate rendezvous point.
(expire : 80 secs)	Hold time remaining until the candidate rendezvous point expires from the mapping agent cache.
224.0.0.0/4	Group range (address and prefix) that the candidate rendezvous point serves.
SM	PIM protocol mode for which this router is advertised as a rendezvous point.
*	Winning rendezvous point for the group range.

Related Commands

Command	Description
auto-rp candidate-rp, on page 257	Configures 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).

show pim bgp-safi

To display multicast distribution tree (MDT) secondary address family (SAFI) entries created in Protocol Independent Multicast (PIM), use the **show pim bgp-safi** command in EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **bgp-safi**

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.

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 3.6.0	This command was introduced.
Release 3.9.0	Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations..

Usage Guidelines

This command has two purposes:

- Creates core SSM trees.
- Resolves RPF path for extranet.

A trigger creates the output displayed when you issue this command:

- The remote PE router uses BGP to advertise the MDT SAFI to PIM.
- PIM creates SAFI entries independently in forward-reference mode to link extranet paths.

Task ID

Task ID	Operations
multicast	read

Examples

The following example shows the output of the **show pim bgp-safi** command:

```
RP/0/RP0/CPU0:router# show pim bgp-safi
grp 226.0.0.1   src 1.1.1.1     rd 1111:1       nexthop 1.1.1.1
grp 226.0.0.2   src 1.1.1.1     rd 111:2        nexthop 1.1.1.1
grp 226.0.0.3   src 1.1.1.1     rd 111:3        nexthop 1.1.1.1
grp 226.0.0.4   src 1.1.1.1     rd 111:4        nexthop 1.1.1.1
grp 226.0.0.5   src 1.1.1.1     rd 111:5        nexthop 1.1.1.1
grp 226.0.0.6   src 1.1.1.1     rd 111:6        nexthop 1.1.1.1
grp 226.0.0.7   src 1.1.1.1     rd 111:7        nexthop 1.1.1.1
grp 226.0.0.8   src 1.1.1.1     rd 111:8        nexthop 1.1.1.1
grp 226.0.0.9   src 1.1.1.1     rd 111:9        nexthop 1.1.1.1
```

For descriptions of the fields in the foregoing output examples, see this table:

Table 31: show pim bgp-safi Field Descriptions

Field	Description
Grp	MDT default group of a multicast VRF (MVRF) acquired from BGP.
Src	MDT source of originating PE router.
RD	MVRF route distinguisher configured in BGP.
Nexthop	BGP next hop of the PE router advertising this SAFI entry.
Ext	Number of extranet paths linked to this SAFI entry.
BGP	Entries created by BGP a remote PE that used BGP to advertise the MDT SAFI to PIM (trigger 1).

show pim bsr candidate-rp

To display Protocol Independent Multicast (PIM) candidate rendezvous point (RP) information for the bootstrap router (BSR), use the **show pim bsr candidate-rp** command in EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **bsr candidate-rp**

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.

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 3.2	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following example shows how to display PIM candidate rendezvous point information:

```
RP/0/RP0/CPU0:router# show pim bsr candidate-rp
PIM BSR Candidate RP Info
```

```
Cand-RP     mode    scope     priority    uptime   group-list
91.1.1.1    SM       16          255      00:00:00     224/4
```

This table describes the significant fields shown in the display.

Table 32: show pim bsr candidate-rp Field Descriptions

Field	Description
Cand-RP	IP address of the candidate BSR rendezvous point.
mode	PIM mode of the candidate BSR rendezvous point.
scope	Number of messages sent.
priority	Candidate BSR rendezvous point priority value.
uptime	Time candidate BSR rendezvous point has been up.

Related Commands

Command	Description
bsr candidate-bsr, on page 264	Configures the router to announce its candidacy as a bootstrap router (BSR).

show pim bsr election

To display Protocol Independent Multicast (PIM) candidate election information for the bootstrap router (BSR), use the **show pim bsr election** command in
EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **bsr election**

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.

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 3.2	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

This example shows how to display PIM candidate election information:

```
RP/0/RP0/CPU0:router# show pim bsr election

PIM BSR Election State

Cand/Elect-State      Uptime     BS-Timer    BSR                C-BSR
```

```
Inactive/Accept-Any   00:00:00   00:00:00    0.0.0.0 [0, 0]   99.1.1.1 [0, 30]
```

This table describes the significant fields shown in the display.

Table 33: show pim bsr election Field Descriptions

Field	Description
Cand/Elect-State	Current candidate BSR state. Possible states include: • No-Info • Not-Elected • Pending • Elected Elect-State indicates the current elected BSR state. Possible states include: • Accept-Any • Accept-Preferred
Uptime	Time the candidate BSR has been up.
BS-Timer	Time remaining before the bootstrap timer fires.
BSR	BSR IP address.
C-BSR	IP address, priority, and hash mask length of the candidate BSR.

Related Commands

Command	Description
bsr candidate-bsr, on page 264	Configures the router to announce its candidacy as a bootstrap router (BSR).

show pim bsr rp-cache

To display Protocol Independent Multicast (PIM) rendezvous point (RP) cache information for the bootstrap router (BSR), use the **show pim bsr rp-cache** command in EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **bsr rp-cache**

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.

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 3.2	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim bsr rp-cache** command:

```
RP/0/RP0/CPU0:router# show pim bsr rp-cache

Group(s) 224.0.0.0/4, RP count 1
RP-addr         Priority    Holdtime(s)   Uptime    Expires
40.40.40.1      255         150           03:05:03  00:02:12
```

This table describes the significant fields shown in the display.

Table 34: show pim bsr rp-cache Field Descriptions

Field	Description
Group(s), RP count	Group range and number of rendezvous points.
RP-addr	IP address of the rendezvous point.
Priority	Priority value of the rendezvous point.
Holdtime(s)	Time the rendezvous point announcement is valid.
Uptime	Time the rendezvous point announcement expires.

Related Commands

Command	Description
bsr candidate-rp, on page 266	Configures the router to advertise itself as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP) to the bootstrap router (BSR).

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**| **ipv6**] **context**

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.

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 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following example illustrates output from use of the **show pim context** command:

```
RP/0/RP0/CPU0:router# show pim  vrf 101 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 35: 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.
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

Field	Description
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).
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 detail

To display detailed information about reverse path forwarding (RPF) tables configured for a VRF context, use the **show pim context detail** command in EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **context detail**

Syntax Description

vrf *vrf-name*	(Optional) Displays a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Displays IPv4 address prefixes.
ipv6	(Optional) Displays IPv6 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 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following sample output shows the default RPF table information in boldface at the end:

```
RP/0/RP0/CPU0:router# show pim ipv6 context detail

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
Not 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 : GigabitEthernet0/5/0/0 (publish pending: F)
Remote MDT Default Group : 0.0.0.0
MDT MTU: 1376
MDT max aggregation: 255
MDT Data Switchover Interval: 30 secs
MDT interface retry count: 0
Virtual interfaces not added in IM
Not registered with MRIB
RIB multipath RPF not enabled
RIB multipath interface not hashed
Not MBGP
OSPF TE not intact
IS-IS TE not intact
Auto RP listen enabled
All interfaces disable operation not done
LPTS sock added
Default granges
Auto RP listen sock added
RPF topology selection route-policy: mt4-p3
Number of Tables: 12 (2 active)
Default RPF Table: IPv4-Unicast-default
   Active, Table ID 0xe0000000
   Registered with ITAL, Registered with RIB
   NSF RIB converged, , NSF RIB converge not received
```

Table 36: show pim context detail 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 IPv6 process would be the table ID of the IPv4 process. In the context of an IPv4 process, the remote table ID would be that of the IPv6 address family.
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 a VRF as registered with Multicast Routing Information Base (MRIB).

Field	Description
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).
Remote MDT Default Group	Identifies the MDT transiting this VRF or address family in use by the remote address family.
MDT MTU	Identifies the maximum transmission unit value of the multicast distribution tree (MDT).
MDT max aggregation	Identifies the maximum MDT aggegation value.
MDT Data Switchover Interval	Identifies the MDT data swichover interval.
MDT interface retry count	Identifies the number of retries by the MDT interface.
Virtual interfaces not added in IM	Identifies the virtual interfaces not added in IM.
Not registered with MRIB	Identifies a VRF as not registered with the Multicast Routing Information Base (MRIB).

Field	Description
RIB multipath RPF not enabled	Signifies that the RIB multipath RPF is not enabled.
RIB multipath interface not hashed	Signifies that the RIB multipath inteface was not hashed.
Not MBGP	Not Multicast Border Gateway protocol.
OSPF TE not intact	Signifies that OSPF protocol traffic engineering is not intact.
IS-IS TE not intact	Signifies that IS-IS protocol traffic engineering is not intact.
Auto RP listen enabled	Signifies that an automatic RP listening socket was enabled.
All interfaces disable operation not done	Signfies that an all interfaces disable operation was not completed.
LPTS sock added	Identifies an LPTS socket added.
Default granges	Identifies the default granges.
Auto RP listen sock added	Signifies that an automatic RP listening socket was added.
RPF topology selection route-policy	Identifies the route policy for RPF topology.
mt4-p3	Flag that indicates that traffic on this route passed a threshold for the data MDT.
Number of Tables	Identifies the number of tables.
Default RPF Table	Identifies the default RPF table.
IPv4-Unicast-default	Identifies the IPv4 unicast default.
Active, Table ID	Identifies the ID of the active table.
Registered with ITAL	Signifies output is registered with ITAL.
Registered with RIB	Signifies output is registered with RIB.
NSF RIB converged	Signifies receipt of NSF RIB convergence.
	Signifies that NSF RIB convergence information was not received.

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**| **ipv6**] **context table**

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.

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 3.7.0	This command was introduced.

Usage Guidelines

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/ RP0 /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 37: 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 df election-state

To display bidirectional designated forwarder (DF) election state for a rendezvous point (RP) or interface, use the **show pim df election-state** command in
EXEC mode

.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **df election-state** [*rp-ip-address*] [*type interface-path-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.
rp-ip-address	(Optional) IP address or name of the rendezvous point. • 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.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X.*
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

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show pim df election-state** command shows the state of DF election on an individual interface or individual rendezvous point (RP) basis. The DF election may result in one of the following states: Offer, Winner, Lose, or Backoff.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim df election-state** command; the far right column shows the interface route metric toward the RP:

```
RP/0/RP0/CPU0:router# show pim df election-state pos 0/4/0/0

RP               Interface              DF State         Timer         Metrics
172.16.1.3        POS0/4/0/0            Winner           7s 956ms      [110/2]
172.16.1.6        POS0/4/0/0            Lose             0s 0ms        [inf/inf]
```

This table describes the significant fields shown in the display.

Table 38: show pim df election-state Field Descriptions

Field	Description
RP	Address of the rendezvous point.
Interface	Interface on which the DF election takes place.
DF State	DF election state for this router: Offer, Winner, Lose, or Backoff.
Timer	Time for which the DF election state is valid.
Metrics	Unicast routing metric for the rendezvous point sent from the DF election.

Related Commands

Command	Description
domain ipv4 host	Defines a static hostname-to-address mapping in the host cache using IPv4. For more information, see *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router*
show pim df winner , on page 346	Displays the bidirectional DF “winner” for a rendezvous point or an interface.

show pim df winner

To display the bidirectional designated forwarder (DF) “winner” for a rendezvous point (RP) or interface, use the **show pim df winner** command in EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **df winner** [*rp-ip-address*] [*type interface-path-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.
rp-ip-address	(Optional) IP address of the rendezvous point: • 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.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X.*
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

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show pim df winner** command displays the DF winner address for each interface or rendezvous point.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show pim df winner** command; the far right column shows the winner metric toward the rendezvous point:

```
RP/0/RP0/CPU0:router# show pim df winner 172.16.1.3

RP               Interface              DF Winner        Metrics
172.16.1.3        Loopback3             172.17.3.2        [110/2]
172.16.1.3        Loopback2             172.17.2.2        [110/2]
172.16.1.3        Loopback1             172.17.1.2        [110/2]
172.16.1.3        POS0/2/0/2             10.10.2.3        [0/0]
172.16.1.3        POS0/2/0/0             10.10.1.2        [110/2]
```

This table describes the significant fields shown in the display.

Table 39: show pim df winner Field Descriptions

Field	Description
RP	Rendezvous point address.
Interface	Interface on which the DF election takes place.
DF Winner	DF winner address.
Metrics	Unicast routing metric for the rendezvous point sent by the DF winner.

Related Commands

Command	Description
domain ipv4 host	Defines a static hostname-to-address mapping in the host cache using IPv4. For more information, see *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router*
show pim df election-state, on page 343	Displays the bidirectional DF election state for a rendezvous point or an 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 EXEC mode.

show pim global summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	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/RP0/CPU0:router# 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 40: 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.
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 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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 address prefixes.
ip-address-name	(Optional) Can be either one of the following: • 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.* • IP address name as defined in the Domain Name System (DNS) hosts table or with the domain **ipv6** host in the form of *X:X::X.*
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 2.0	This command was introduced.
Release 3.2	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 41: 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 *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router*
rp-address, on page 313	Configures the address of a PIM rendezvous point for a particular group.
show pim range-list, on page 370	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**| **ipv6**] **interface** [*type interface-path-id*| **state-on**| **state-off**] **[detail]**

Syntax Description

	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 42: 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.

Field	Description
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.
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 365	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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 43: 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 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 4.3.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read

Examples

The following sample output from the **show pim rpf-redirect** command displays statistics about the PIM bundles:

```
RP/0/RP0/CPU0:router#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 4.3.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read

show pim mdt

To display information about data multicast distribution tree (MDT) streams, use the **show pim mdt** command in EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **mdt** {**cache** [*ip-address*| **detail**| **summary**]| **interface**| **prefix** [**local**| **remote**]}

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.
cache	Displays those data-MDT streams currently running and in the cache.
ip-address	(Optional) Specifies the core source IP address or name, or both, for the data MDT streams: • 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.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X.*
detail	Displays detailed cache information.
summary	(Optional) Displays a summary of the data MDT cache.
interface	(Optional) Displays the default MDT interface.
prefix	Displays the local or remote prefixes that can be or have been used.
local	(Optional) Specifies locally assigned data MDT prefixes.
remote	(Optional) Specifies data MDT prefixes learned from remote PE routers.

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 3.6.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following example shows how to display PIM candidate rendezvous point information:

```
RP/0/RP0/CPU0:router# show pim vrf svpn20 mdt cache

Core Source      Cust (Source, Group)                Core Group       Expires
2.2.2.2          (204.161.20.1, 226.1.1.1)           232.1.20.53      00:02:18
2.2.2.2          (204.161.20.1, 226.1.1.2)           232.1.20.52      00:02:18

RP/0/RP0/CPU0:router# show pim vrf all mdt interface

GroupAddress
Interface
Source
Vrf
239.1.1.1
mdt101
Loopback1
101
239.1.1.2
mdt102
Loopback2
102
239.1.1.3
mdt102
Loopback0
103
```

Table 44: show pim mdt Field Descriptions

Field	Description
Core Source	Specifies the core source IP address or name, or both, for the data MDT streams.
Cust (Source, Group)	Specifies the actual multicast traffic source and group address from a customer site.
Core Group	Specifies the core group IP address.
Expires	Time at which data MDT expires.

show pim mstatic

To display multicast static routing information, use the **show pim mstatic** command in EXEC

mode.

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

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 3.4.0	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/RP0/CPU0:router# 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 45: 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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show pim neighbor** command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# 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/RP0/CPU0:router# 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 46: 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.
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.
Bidir	Indicates that the neighbor is capable of bidirectional PIM mode operation.
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 353	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.
ipv6	(Optional) Specifies IPv6 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.

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/RP0/CPU0:router# 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 47: 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.
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**| **ipv6**] **range-list** [**autorp**| **config**] [*ip-address-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.
autorp	(Optional) Displays PIM auto-rendezvous point (Auto-RP) range list information.
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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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 48: 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 350	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**| **ipv6**] {**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.
ipv6	(Optional) Specifies IPv6 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 : • 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.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X.* **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 3.7.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
multicast	read

Examples

The following example shows output from the **show pim rpf** command:

```
RP/0/RP0/CPU0:router# 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**| **ipv6**] [**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.
ipv6	(Optional) Specifies IPv6 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 as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X* .
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). • If **ipv4** is specified, the range in bit length is 0 to 32. • If **ipv6** is specified, the range in bit length is 0 to 128. **Note** Not a valid keyword for IPv6 unicast domain names.
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 3.3.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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/RP0/CPU0:router# 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/RP0/CPU0:router# 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 372	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**| **ipv6**] **rpf route-policy statistics**

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.

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 3.7.0	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# 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 49: 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.
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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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: • 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.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X.*

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 3.7.0	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# 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 50: 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**| **ipv6**] [**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.
ipv6	(Optional) Specifies IPv6 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 3.7.0	This command was introduced.

Usage Guidelines

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/RP0/CPU0:router# 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/RP0/CPU0:router# 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 EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** keyword and *vrf-name* argument were added.

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/RP0/CPU0:router# 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 51: 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 table-context

To display detailed information about multitopology tables, use the **show pim table-context** command in EXEC mode.

show pim [**vrf** *vrf-name*] [**ipv4**| **ipv6**] [**unicast**| **multicast**| **safi-all**] [**topology** {*table-name*| **all**}] **table-context**

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.
unicast	(Optional) Specifies a unicast secondary address family (SAFI).
multicast	(Optional) Specifies a multicast secondary address family (SAFI).
safi-all	(Optional) Specifies a secondary address family (SAFI) wildcard.
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 3.7.0	This command was introduced.

Usage Guidelines

Examples

The following sample output shows the PIM table contexts for a VRF default:

```
RP/0/RP0/CPU0:router# show pim table-context

PIM Table contexts for VRF default

Table: IPv4-Unicast-default
```

```
    Active, Table ID 0xe0000000, VRF ID 0x60000000
    Registered with ITAL, Registered with RIB
    NSF RIB converged, NSF RIB converge not received
    Number of RPF monitors 1

Table: IPv4-Multicast-default
    Active, Table ID 0xe0100000, VRF ID 0x60000000
    Registered with ITAL, Registered with RIB
    NSF RIB converged, NSF RIB converge not received
    Number of RPF monitors 0

Description:  A Table is considered to be "active" when it is globally configured under a
given VRF and RSI considers it to be active (and the same is notified to PIM by ITAL). The
 opposite of this means the Table is "inactive".
```

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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 address prefixes.
src-ip-address/ grp-address	Source IP address or group IP address, or both, for the default or selected route policy: • 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.* • IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv6 host in the form of *X:X::X.*

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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added. The *name* and *ip-address* arguments were combined to be *ip-address* .
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added. The *ip-address* argument was changed to *source-ip-address* [*group-ip-address*].

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 393.

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/RP0/CPU0:router# 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/RP0/CPU0:router# 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
```

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 52: 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).

Field	Description
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
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.

Field	Description
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.
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).

Field	Description
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**| **ipv6**] **topology detail**

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.

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 3.7.0	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/RP0/CPU0:router# 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/RP0/CPU0:router# 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
```

Table 52: show pim topology Field Descriptions, on page 389 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 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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 3.4.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.
Release 3.7.0	The **detail** and **route-count** keywords were added.

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/RP0/CPU0:router# 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
```

Table 52: show pim topology Field Descriptions, on page 389 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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 3.4.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.
Release 3.7.0	The **detail** and **route-count** keywords were added.

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/RP0/CPU0:router# 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
```

Table 52: show pim topology Field Descriptions, on page 389 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**| **ipv6**] **topology summary [detail]**

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.
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 3.4.0	This command was introduced.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.
Release 3.6.0	The *detail* argument was added.

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/RP0/CPU0:router# 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 393.

show pim traffic

To display Protocol Independent Multicast (PIM) traffic counter information, use the **show pim traffic** command in EXEC mode .

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.

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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

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/RP0/CPU0:router# 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 53: 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.

Field	Description
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 272	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**| **ipv6**] **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.
ipv6	(Optional) Specifies IPv6 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 2.0	This command was introduced.
Release 3.4.0	The **ipv4** and **ipv6** keywords were added. The **netio** keyword was added.
Release 3.5.0	The **vrf** *vrf-name* keyword and argument were added.

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) and bidirectional PIM.

Task ID

Task ID	Operations
multicast	read

Examples

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

```
RP/0/RP0/CPU0:router# 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 54: 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.

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 2.0	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/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(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 2.0	This command was introduced.
Release 3.3.0	The **default-range** keyword was deleted.
Release 3.4.0	The **allow-override** keyword was added.
Release 3.5.0	This command was introduced in multicast VPN configuration mode. The *access-list* argument was changed from optional to required.

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/RP0/CPU0:router(config)# ipv4 access-list 4
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 224.2.151.141
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# ssm range 4
```

Multicast Tool and Utility Commands

This chapter describes the commands used to troubleshoot multicast routing sessions on Cisco IOS XR Software.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Implementing Multicast Routing on the Cisco IOS XR Software* in *Cisco IOS XR Multicast Configuration Guide for the Cisco CRS Router*.

- mrinfo, page 414
- mtrace, page 416
- sap cache-timeout, page 418
- sap listen, page 419
- show sap, page 421

mrinfo

To query neighboring multicast routers peering with the local router, use the **mrinfo** command in EXEC mode.

mrinfo [ipv4] *host-address* [*source-address*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
host-address	Can be either the Domain Name System (DNS) name or IP address of a multicast router entered in *A.B.C.D* format. **Note** If omitted, the router queries itself.
source-address	(Optional) Source address used on multicast routing information (mrinfo) requests. If omitted, the source is based on the outbound interface for the destination.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.5.0	The *host-address* argument was changed from optional to required.

Usage Guidelines

The **mrinfo** command determines which neighboring multicast routers are peering with a multicast router.

You can query a multicast router with this command. The output format is identical to the multicast routed version of Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Task ID

Task ID	Operations
multicast	execute

Examples

The following is sample output from the **mrinfo** command. The first line shows the multicast configuration with version number and flags Parent Multicast Agent (PMA). The flags mean that the configuration is prune capable, mtrace capable, and SNMP capable. For each neighbor of the queried multicast router, the IP address of the queried router is displayed, followed by the IP address of the neighbor. The metric (cost of connect) and the threshold (multicast time to live) are displayed. Other information is available, such as whether this router is

- Running the PIM protocol
- An IGMP querier
- A leaf router

```
RP/0/RP0/CPU0:router# mrinfo 192.168.50.1

192.168.50.1 [version  0.37.0] [flags: PMA]:
  172.16.1.1 -> 172.16.1.1 [1/0/pim/querier/leaf]
  172.16.2.2 -> 172.16.2.2 [1/0/pim/querier/leaf]
  192.168.50.1 -> 192.168.50.1 [1/0/pim/querier]
  192.168.50.1 -> 192.168.50.101 [1/0/pim/querier]
  192.168.40.101 -> 192.168.40.1 [1/0/pim]
  192.168.40.101 -> 192.168.40.101 [1/0/pim]
```

mtrace

To trace the path from a source to a destination branch for a multicast distribution tree, use the **mtrace** command in EXEC mode.

mtrace [ipv4] [vrf] *source destination* [*group_addr*] *[resp_addr]*[*ttl*]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
vrf	(Optional) Specifies the vrf table for the route lookup.
source	Domain Name System (DNS) name or the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.
destination	DNS name or address of the unicast destination. This is a unicast address of the end of the path to be traced.
group_addr	(Optional) DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for MBONE Audio). When address 0.0.0.0 is used, the software invokes a *weak mtrace*. A weak mtrace is one that follows the Reverse Path Forwarding (RPF) path to the source, regardless of whether any router along the path has multicast routing table state.
resp_addr	(Optional) DNS name or multicast address of the response address to receive response.
ttl	(Optional) Time-to-live (TTL) threshold for a multicast trace request. Range is 1 to 255 router hops.

Command Default

By default, this feature is disabled.

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The trace request generated by the **mtrace** command is multicast to the multicast group to find the last-hop router to the specified destination. The trace follows the multicast path from destination to source by passing

the mtrace request packet using unicast to each hop. Responses are unicast to the querying router by the first-hop router to the source. This command allows you to isolate multicast routing failures.

If no arguments are entered, the router interactively prompts you for them.

This command is identical in function to the UNIX version of **mtrace**.

Task ID

Task ID	Operations
multicast	execute

Examples

The following is sample output from the **mtrace** command:

```
RP/0/RP0/CPU0:router# mtrace 172.16.1.0 172.16.1.10 239.254.254.254

Type escape sequence to abort.
Mtrace from 172.16.1.0 to 172.16.1.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...

Switching to hop-by-hop:
0  172.16.1.10
-1  172.17.20.101 PIM Reached RP/Core [172.16.1.0/24]
-2  172.18.10.1 PIM  [172.16.1.0/32]
-3  172.16.1.0 PIM  [172.16.1.0/32]

RP/0/RP0/CPU0:router# mtrace vrf vrf1 172.16.1.0 172.16.1.10 239.254.254.254 45.244.244.244
 49
```

sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the **sap cache-timeout** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

sap cache-timeout *minutes*

no sap cache-timeout

Syntax Description

minutes	Time that a SAP cache entry is active in the cache. Range is 1 to 1440.

Command Default

minutes : 1440 (24 hours)

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **sap cache-timeout** command defines how long session announcements are cached by the router. Active session announcements are periodically re-sent by the originating site, refreshing the cached state in the router. The minimum interval between announcements for a single group is 5 minutes. Setting the cache timeout to a value less than 30 minutes is not recommended. Set the cache timeout to 0 to keep entries in the cache indefinitely.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example shows the SAP cache entry timeout being configured at 10 minutes:

```
RP/0/RP0/CPU0:router(config)# sap cache-timeout 10
```

sap listen

To configure the Session Announcement Protocol (SAP) designated router (SDR) listener on a group address, use the **sap listen** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

sap listen [*ip-address*| *name*]

no sap listen

Syntax Description

ip-address	(Optional) Group IP address for an address range.
name	(Optional) Name of a prefix for an address range.

Command Default

When no group address is configured, the SDR listener is configured on the global SAP announcement group (224.2.127.254).

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **sap listen** command configures an SDR listener that listens to SAP announcements on the configured group address. The group IP address can be any group in the range from 224.2.128.0 to 224.2.255.255.

Task ID

Task ID	Operations
multicast	read, write

Examples

The following example configures an SDR listener for group on IP address 224.2.127.254:

```
RP/0/RP0/CPU0:router(config)# sap listen 224.2.127.254
```

Related Commands

Command	Description
show sap, on page 421	Displays the SAP sessions learned on the configured multicast groups.

show sap

To display the Session Announcement Protocol (SAP) sessions learned on the configured multicast groups, use the **show sap** command in
EXEC mode

.

show sap [ipv4] [*group-address*| *session-name*] **[detail]**

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
group-address	(Optional) Group IP address or name of the session that is learned.
session-name	(Optional) Session name.
detail	(Optional) Provides more SAP information.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **show sap** command displays the sessions learned on the configured multicast groups. The **detail** keyword displays verbose session information.

Use the **sap listen** command to configure the SDR listener on a group IP address.

Task ID

Task ID	Operations
multicast	read

Examples

The following is sample output from the **show sap** command. Information is summarized and shows one entry.

```
RP/0/RP0/CPU0:router# show sap
```

```
Sap Session Table Summary
Cisco Systems, Inc
Src: 192.168.30.101, Dst: 224.2.127.254, Last Heard: 00:00:23
Total Entries : 1
```

This table describes the significant fields shown in the display.

Table 55: show sap Field Descriptions

Field	Description
Src	IP address of the host from which this session announcement was received.
Dst	Destination IP multicast group address where the announcement was sent.
Last Heard	Time (in hours, minutes, and seconds) when SAP announcements were last heard from the source.
Total Entries	Total number of entries displayed.

The following is sample output from the **show sap** command with the **detail** keyword specified for the SAP session, Cisco Systems, Inc.

```
RP/0/RP0/CPU0:router# show sap detail

Sap Session Table
Session Name: Cisco Systems, Inc
Description: IPTV Streaming Video
Group: 225.225.225.1 TTL: 2
Announcement source: 192.30.30.101, Destination: 224.2.127.254
Created by: - 0050c200aabb 9 IN IP4 10.10.176.50
Session Permanent Attribute: packetsize:4416
Attribute: packetformat:RAW
Attribute: mux:m1s
Attribute: keywds:
Attribute: author:Cisco Systems, Inc
Attribute: copyright:Cisco Systems, Inc
Media : video, Transport Protocol : udp, Port : 444
Total Entries : 1
```

This table describes the significant fields shown in the display.

Table 56: show sap detail Field Descriptions

Field	Description
Session Name	Descriptive name of the SAP session.
Description	An expanded description of the session.
Group	IP multicast group addresses used for this session.
Announcement source	IP address of the host from which this session announcement was received.

Field	Description
Destination	Destination IP multicast group address that the announcement was sent to.
Created by	Information for identifying and tracking the session announcement.
Attribute	Indicates attributes specific to the session.
Media	Indicates the media type (audio, video, or data), transport port that the media stream is sent to, transport protocol used for these media (common values are User Datagram Protocol [UDP] and Real-Time Transport Protocol [RTP]/AVP), and list of media formats that each media instance can use. The first media format is the default format. Format identifiers are specific to the transport protocol used.

Related Commands

Command	Description
sap listen, on page 419	Configures the SDR listener on a group IP address.

Automatic Multicast Tunneling Commands

This module describes the commands used to configure Automatic Multicast Tunneling (AMT) on the Cisco IOS XR Software.

For detailed information regarding AMT, refer the *Cisco IOS XR Multicast Configuration Guide for the Cisco CRS Router*.

- advertisement-address, page 426
- clear mfib counter amt, page 427
- gateway-filter, page 428
- maximum gateway, page 429
- maximum route, page 430
- maximum route-gateway, page 431
- mtu (amt), page 432
- router amt relay ipv4, page 433
- qqic, page 434
- show amt gateway, page 435
- show amt summary, page 436
- show mrib amt gateway, page 437
- show mrib amt route, page 440
- tos(amt), page 442
- ttl(amt), page 443

advertisement-address

To specify the unique relay address for an Automatic Multicast Tunneling (AMT) process, use the **advertisement-address** command in the AMT relay configuration mode. To remove the specified address, use the **no** form of the command.

advertisement-address *relay-address*

no advertisement-address

Syntax Description

relay address	Interface address.

Command Default

None

Command Modes

AMT relay configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

The below example shows how to use the **advertisement-address** command:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # advertisement-address 1.1.1.1 pos 5/1/0/0
```

Related Commands

Command	Description
router amt relay ipv4, on page 433	Enables Automatic Multicast Tunneling (AMT).

clear mfib counter amt

To clear the Automatic Multicast tunneling (AMT) statistics, use the **clear mfib counter amt** command in the EXEC mode.

clear mfib counter amt *location*

Syntax Description

location	AMT location.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
amt	read, write

Examples

```
RP/0/RP0/CPU0:router # clear mfib counter amt gig 0/1/2/0
```

gateway-filter

To enable the configured Access Lists (ACLs) to allow/ drop specific gateways, use the **gateway-filter** command in the AMT relay configuration mode. To disable this feature, use the **no** form of the command.

gateway-filter *acl-name*

no gateway-filter

Syntax Description

acl-name	Displays the defined ACL name.

Command Default

None

Command Modes

AMT relay configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

IPv6 ACLs are not supported.

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to run the **gateway-filter** command:

```
RP/0/RP0/CPU0:router (config-amt-v4-relay) # gateway-filter a1
```

maximum gateway

To restrict the total number of Automatic Multicast Tunneling (AMT) gateways in the IGMP/ MLD process, use the **maximum gateway** command in the AMT relay configuration mode. To remove the defined limit, use the **no** form of the command.

maximum gateway *value*

no maximum gateway *value*

Syntax Description

value	Maximum number of gateways. Range is from 0 to 4294967295.

Command Default

Default value is 10000.

Command Modes

AMT relay configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to configure the maximum gateway to 5000:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # maximum gateway 5000
```

maximum route

To restrict the number of routes per Automatic Multicast Tunneling (AMT) gateway, use the **maximum route** command in the AMT relay configuration mode. To remove the defined maximum route value, use the **no** form of the command.

maximum route ipv4 | ipv6 *value*

nomaximum route

Syntax Description

IPv4 | IPv6	Defines the maximum route for the selected address-family.
value	Maximum route value. Range is from 0 to 4294967295.

Command Default

Default value is 1000.

Command Modes

AMT relay configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to define the maximum route to 500:

```
RP/0/RP0/CPU0:router (config-amt-relay-ipv4) # maximum route ipv4 500
```

maximum route-gateway

To restrict the number of route-gateways (tunnels), use the **maximum route-gateway** command in the AMT configuration mode. To remove the defined maximum route-gateways, use the **no** form of the command.

maximum route-gateway{ ipv4 | ipv6 } *value*

no maximum route-gateway

Syntax Description

ipv4 | ipv6	Defines the maximum route-gateways for the selected address-family.
value	Maximum route-gateway value. The rRange is from 0 to 4294967295.

Command Default

Default value is 10000.

Command Modes

AMT relay configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to configure the maximum route-gateway to 500:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # maximum route-gateway 500
```

Related Commands

Command	Description
maximum gateway, on page 429	Restricts the total number of Automatic Multicast Tunneling (AMT) gateways, in the IGMP/ MLD process.
gateway-filter, on page 428	Enables the configured Access Lists (ACLs) to allow or drop specific gateways.
maximum route, on page 430	Restricts the number of routes per Automatic Multicast Tunneling (AMT) gateway.

mtu (amt)

To set the Maximum Transmission Units for Automatic Multicast Tunneling (AMT), use the **mtu**in the AMT configuration mode. To delete the set value, use the **no** form of the command.

mtu *value*

no mtu

Syntax Description

value	Specifies the MTU value.

Command Default

9000

Command Modes

AMT configuration mode.

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to use the **mtu** command:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # mtu 1000
```

router amt relay ipv4

To enable the Automatic Multicast Tunneling (AMT) process, use the **router amt relay ipv4** command in the global configuration mode. To remove all the AMT configurations, use the **no** form of the command.

router amt relay ipv4

no router amt relay ipv4

Syntax Description

This command has no keywords or arguments.

Command Default

No AMT sessions are created.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

This command enables IPv4 AMT relay submode. IPv6 tunneling is currently not available.

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to enable the router amt command:

```
RP/0/RP0/CPU0:router (config) # router amt relay ipv4
```

qqic

To set the Querier's Query Interval Code (QQIC) value for the Automatic Multicast Tunneling (AMT) membership query message, use the **qqic** command in the AMT configuration mode. To remove the set QQIC value, use the **no** form of the command.

qqic *qqic-value*

no qqic *qqic-value*

Syntax Description

qqic-value	QQIC value. Range is from 0 to 4294967295.

Command Default

Default value is 1000.

Command Modes

AMT configuration mode

Command History

Release	Modification
Release 4.3.1	

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to define the qqic value to 500:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # qqic 500
```

Related Commands

Command	Description
router amt relay ipv4, on page 433	Enables Automatic Multicast Tunneling (AMT).

show amt gateway

To display the gateway details for Automatic Multicast Tunneling, use the **show amt gateway** command in the EXEC mode.

show amt gateway *gateway-address port*

Syntax Description

gateway-address	Specifies the gateway address in the R/S/I/P format.
port	Specifies the gateway port. The range is from 0 to 4294967295.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read

Examples

This example shows how to run the **show amt gateway** command:

```
show amt gateway 13.1.1.2 3000
13.1.1.2/3000
    Keylen: 48, nonce: 0xf44dfd23, nh: 192.11.11.2
    UPD    : 2340 / 0
```

Related Commands

Command	Description
show amt summary, on page 436	Displays Automatic Multicast Tunneling information in brief.

show amt summary

To display the configured Automatic Multicast Tunneling details in brief, use the **show amt summary** command in EXEC mode.

show amt summary { ipv4 | ipv6}

Syntax Description

ipv4 | ipv6	Displays IPv4 / IPv6 AMT information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read

Examples

The following example shows the IPv4 AMT details:

```
show amt ipv4 summary
Anycast-prefix     : 50.1.0.0/16, GW-SIM: False
Relay Adv-Addr     : 1.1.1.1
  MTU/TOS/TTL/QQIC : 1500/2/20/60
  GW count: 64, Max: 64000
  Route Count: 0/1000, Tunnels: 64000/64000
  ACL: 0, OOR: 1
```

Related Commands

Command	Description
router amt relay ipv4, on page 433	Enables Automatic Multicast Tunneling (AMT).

show mrib amt gateway

To display the Multicast Routing Information Base (mrib) gateway details for the Automatic Multicast Tunneling process, use the **show mrib amt gateway** command in the EXEC mode.

show mrib amt gateway [*port-value* | *gateway-address*] [**expired** | **summary**]

Syntax Description

summary	Displays the AMT gateway summary.
expired	Displays the expired AMT gateways.
port-value	Gateway details for the specified port. Range for the port value is from 1 to 1048575.
gateway-address	Gateway details for the specified address.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read

Examples

This example shows how to use the **show mrib amt gateway** command:

```
show mrib amt gateway
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, MoFP - MoFRR Primary
    MoFB - MoFRR Backup
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept
(13.1.1.2,3000)
  Source/Group:(195.1.1.2,232.1.4.232)
    Joined at: 00:04:01
    Total Packets/Bytes Sent: 2092/3100344
  Source/Group:(195.1.1.2,232.1.4.231)
    Joined at: 00:04:01
    Total Packets/Bytes Sent: 2092/3100344
  Source/Group:(195.1.1.2,232.1.4.230)
    Joined at: 00:04:01
    Total Packets/Bytes Sent: 2092/3100344
  Source/Group:(195.1.1.2,232.1.4.229)
    Joined at: 00:04:01
    Total Packets/Bytes Sent: 2092/3100344
  Source/Group:(195.1.1.2,232.1.4.228)
    Joined at: 00:04:01
    Total Packets/Bytes Sent: 2092/3100344
```

This example shows how to use the **show mrib amt gateway** command with the **summary** keyword:

```
show mrib amt gateway summary
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, MoFP - MoFRR Primary
    MoFB - MoFRR Backup
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept
(13.1.1.2,3000)
    Number of Multicast streams (S,G)joined: 1000
    Total Packets/Bytes Sent [Acitve route]: 1823891/2703006462
    Total Packets/Bytes Sent [Expired route]: 160775898/238268611218
(13.1.1.3,3000)
    Number of Multicast streams (S,G)joined: 1000
    Total Packets/Bytes Sent [Acitve route]: 1784325/2644369650
    Total Packets/Bytes Sent [Expired route]: 160936848/238507137712
```

This example shows how to use the **show mrib amt gateway** command with the **expired** keyword:

```
show mrib amt gateway expired
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, MoFP - MoFRR Primary
    MoFB - MoFRR Backup
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept
(13.1.1.2,3000)
  Source/Group:(195.1.1.2,232.1.4.232)
    Joined at: 05:34:59
    Total Packets/Bytes Sent: 160948/238524936
```

```
  Source/Group:(195.1.1.2,232.1.4.231)
    Joined at: 05:34:59
    Total Packets/Bytes Sent: 160948/238524936
```

This example shows how to use the **show mrib amt gateway** command with port value specified at 3000:

```
show mrib amt gateway 3000
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, MoFP - MoFRR Primary
    MoFB - MoFRR Backup
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept
(13.1.1.2,3000)
  Source/Group:(195.1.1.2,232.1.4.232)
    Joined at: 00:07:40
    Total Packets/Bytes Sent: 4121/6107322
  Source/Group:(195.1.1.2,232.1.4.231)
    Joined at: 00:07:40
    Total Packets/Bytes Sent: 4121/6107322
```

show mrib amt route

To display the Multicast Routing Information Base (mrib) route details, use the **show mrib amt route** command in the EXEC mode.

show mrib amt route *source-address* [**expired** | **summary**]

Syntax Description

summary	Displays the AMT route summary.
expired	Displays the expired AMT routes.
source-address	Route details for the specified source address.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read

Examples

This example shows how to use the **show mrib amt route** command:

```
show mrib amt route
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, MoFP - MoFRR Primary
    MoFB - MoFRR Backup
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept
```

```
(195.1.1.2,232.1.1.1)
  AMT Tunnel: GW: 13.1.1.2/3000, TenGigE0/0/0/2 Flags: AT, Up: 00:05:13
              Src:1.1.1.1, NH: 192.11.11.2, AMT-ID: 662986
              Total Packets/Bytes Sent: 2758/4087356
  AMT Tunnel: GW: 13.1.1.3/3000, TenGigE0/0/0/2 Flags: AT, Up: 00:05:10
              Src:1.1.1.1, NH: 192.11.11.2, AMT-ID: 681670
              Total Packets/Bytes Sent: 2727/4041414
```

This example shows how to use the **show mrib amt route** command with the **summary** keyword:

```
show mrib amt route summary
(195.1.1.2,232.1.1.1)
  Number of AMT Gateways currently joined: 64
  Total Packets/Bytes out [Active]: 10253760 / 15195982336
  Total Packets/Bytes out [Expired]: 0 / 0

(195.1.1.2,232.1.1.2)
  Number of AMT Gateways currently joined: 64
  Total Packets/Bytes out [Active]: 10253760 / 15195982336
  Total Packets/Bytes out [Expired]: 0 / 0
```

This example shows how to use the **show mrib amt route** command with the **expired** keyword:

```
show mrib amt route expired
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, MoFP - MoFRR Primary
    MoFB - MoFRR Backup
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept
(195.1.1.2,232.1.1.1)
  AMT Tunnel: ID: 586786 GW: 13.1.1.2/3000
    Joined at: 05:28:08
    Expired at: 00:00:08
    Total Packets/Bytes Sent: 160870/238407934
```

tos(amt)

To set the Type of Service (TOS) value for Automatic Multicast Tunneling (AMT), use the **tos** command in the AMT configuration mode. To delete the set TOS value, use the **no**form of the command.

tos *value*

no tos

Syntax Description

value	TOS value. Range is from 1 to 255.

Command Default

1

Command Modes

AMT configuration mode.

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to use the **tos** command:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # tos 5
```

ttl(amt)

To set the Time To Live (TTL) value for Automatic Multicast Tunneling (AMT), use the **ttl** command in the AMT configuration mode. To delete the set TTL value, use the **no**form of the command.

ttl *value*

nottl

Syntax Description

value	Specifies the TTL value.

Command Default

255 ms

Command Modes

AMT configuration mode.

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
multicast	read, write

Examples

This example shows how to use the **ttl** command:

```
RP/0/RP0/CPU0:router (config-amt-relay-v4) # ttl 500
```