



## **Multicast Command Reference for the Cisco NCS 6000 Series Router, Release 5.0.x**

### **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

Text Part Number: OL-





## CONTENTS

---

### Preface

### Preface ix

Changes to this Document ix

Obtaining Documentation and Submitting a Service Request ix

---

### CHAPTER 1

### 1

access-group (IGMP) 3

clear igmp counters 5

clear igmp group 7

clear igmp reset 9

explicit-tracking 11

join-group 13

maximum groups 15

maximum groups-per-interface 17

20

query-interval 22

query-max-response-time 24

query-timeout 26

robustness-count 28

router 29

router igmp 31

show igmp groups 33

show igmp interface 35

show igmp nsf 39

show igmp summary 41

show igmp ssm map 44

show igmp traffic 46

ssm map static 50

static-group 52  
 version 54  
 vrf (igmp) 56

---

## CHAPTER 2

### Multicast Source Discovery Protocol Commands on 57

cache-sa holdtime 59  
 cache-sa-state 61  
 clear msdp peer 63  
 clear msdp sa-cache 65  
 clear msdp stats 67  
 connect-source 69  
 default-peer 71  
 description (peer) 73  
 maximum external-sa 75  
 maximum peer-external-sa 77  
 mesh-group (peer) 79  
 originator-id 81  
 password (peer) 83  
 peer (MSDP) 85  
 remote-as (multicast) 87  
 sa-filter 88  
 show msdp globals 90  
 show msdp peer 93  
 show msdp rpf 96  
 show msdp sa-cache 98  
 show msdp statistics peer 103  
 show msdp summary 105  
 shutdown (MSDP) 107  
 ttl-threshold (MSDP) 109

---

## CHAPTER 3

### Multicast Routing and Forwarding Commands on 111

accounting per-prefix 113  
 accounting per-prefix forward-only 115  
 address-family (multicast) 117  
 boundary 120

[clear mfib counter](#) 121

[clear mfib database](#) 123

[clear mfib hardware adjacency-counters](#) 124

[disable \(multicast\)](#) 125

[enable \(multicast\)](#) 127

[forwarding-latency](#) 129

[interface \(multicast\)](#) 131

[interface all enable](#) 133

[interface-inheritance disable](#) 135

[log-traps](#) 137

[maximum disable](#) 138

[mdt data](#) 139

[mdt default](#) 141

[mdt mtu](#) 143

[mdt source](#) 145

[mhost default-interface](#) 147

[multicast-routing](#) 149

[nsf \(multicast\)](#) 151

[oom-handling](#) 153

[rate-per-route](#) 155

[show mfib connections](#) 156

[show mfib counter](#) 158

[show mfib encap-info](#) 160

[show mfib hardware route accept-bitmap](#) 162

[show mfib hardware route olist](#) 164

[show mhost default-interface](#) 166

[show mhost groups](#) 168

[show mrrib client](#) 170

[show mrrib nsf](#) 173

[show mrrib route](#) 175

[show mrrib route-collapse](#) 177

[show mrrib route outgoing-interface](#) 179

[show mrrib table-info](#) 181

[show mrrib tlc](#) 183

[ttl-threshold \(multicast\)](#) 185

vrf (multicast) 187

## CHAPTER 4

### Multicast PIM Commands on 189

accept-register 191

auto-rp candidate-rp 193

bsr-border 196

bsr candidate-bsr 198

bsr candidate-rp 200

clear pim counters 202

clear pim topology 205

dr-priority 207

global maximum 209

hello-interval (PIM) 211

interface (PIM) 213

join-prune-interval 215

maximum register-states 217

maximum route-interfaces 219

maximum routes 221

mofrr 223

neighbor-check-on-recv enable 225

neighbor-check-on-send enable 226

neighbor-filter 227

nsf lifetime (PIM) 228

old-register-checksum 230

router pim 232

rp-address 234

rpf topology route-policy 236

rpf-vector 238

rp-static-deny 239

show auto-rp candidate-rp 240

show pim context 242

show pim context table 245

show pim group-map 247

show pim interface 249

show pim join-prune statistic 252

[show pim mstatic](#) 254  
[show pim neighbor](#) 256  
[show pim nsf](#) 259  
[show pim range-list](#) 261  
[show pim summary](#) 263  
[show pim topology](#) 265  
[show pim topology detail](#) 271  
[show pim topology entry-flag](#) 274  
[show pim topology interface-flag](#) 277  
[show pim topology summary](#) 280  
[show pim traffic](#) 282  
[show pim tunnel info](#) 285  
[spt-threshold infinity](#) 287  
[ssm](#) 288

---

**CHAPTER 5****Multicast Tool and Utility Commands on** 291

[mrinfo](#) 292  
[mtrace](#) 294  
[sap cache-timeout](#) 296  
[sap listen](#) 297  
[show sap](#) 299







## Preface

---

The Preface contains these topics:

- [Changes to this Document, page ix](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

## Changes to this Document

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

**Table 1: Changes to This Document**

Revision	Date	Change Summary
OL-30981-01	November 2013	Initial release of this document.

## 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*, at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.





---

This chapter describes the commands used to configure and monitor IPv4 .

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 *Multicast Configuration Guide for Cisco NCS 6000 Series Routers* .

- [access-group \(IGMP\), page 3](#)
- [clear igmp counters, page 5](#)
- [clear igmp group, page 7](#)
- [clear igmp reset, page 9](#)
- [explicit-tracking, page 11](#)
- [join-group, page 13](#)
- [maximum groups, page 15](#)
- [maximum groups-per-interface, page 17](#)
- [, page 20](#)
- [query-interval, page 22](#)
- [query-max-response-time, page 24](#)
- [query-timeout, page 26](#)
- [robustness-count, page 28](#)
- [router, page 29](#)
- [router igmp, page 31](#)
- [show igmp groups, page 33](#)
- [show igmp interface, page 35](#)
- [show igmp nsf, page 39](#)
- [show igmp summary, page 41](#)
- [show igmp ssm map, page 44](#)
- [show igmp traffic, page 46](#)
- [ssm map static, page 50](#)

- [static-group](#), page 52
- [version](#), page 54
- [vrf \(igmp\)](#), page 56

## access-group (IGMP)

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

**access-group** *access-list*

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

<b>Syntax Description</b>	<i>access-list</i> Number or name of a standard IP access list. Range is 1 to 99.	
<b>Command Default</b>	No default behavior or values	
<b>Command Modes</b>	IGMP interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.
<b>Usage Guidelines</b>	<p>To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.</p> <p>If this command is not specified in router Internet Group Management Protocol (IGMP) configuration mode, the interface accepts all multicast join requests by hosts.</p>	
<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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
```

**Related Commands**

Command	Description
<b>ipv4 access-list</b>	Defines a standard IP access list. For information, see <i>IP Addresses and Services Configuration Guide for Cisco NCS 6000 Series Routers</i>

# 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

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

## Command Default

No default behavior or values

## Command Modes

EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show igmp traffic, on page 46</a>	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

<b>ipv4</b>	(Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<i>ip-address</i>	(Optional) IP hostname or group address.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show igmp groups, on page 33</a>	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

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

## Command Default

No default behavior or values

## Command Modes

EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show igmp groups, on page 33</a>	Displays the multicast groups that are directly connected to the router and that were learned through IGMP
<b>show mrib route</b>	Displays all route entries in the MRIB table.

# explicit-tracking

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

**explicit-tracking** [*access-list*] **disable**

**no explicit-tracking**

## Syntax Description

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

## Command Default

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

## Command Modes

IGMP VRF configuration  
IGMP interface configuration  
MLD configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

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

**Note**

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

```
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
<a href="#">show igmp groups, on page 33</a>	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

# join-group

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

**join-group** *group-address* [ *source-address* ]

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

## Syntax Description

<i>group-address</i>	Address of the multicast group. This is a multicast IP address group in IPv4 format <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i> .</li> </ul>
<i>source-address</i>	(Optional) Source address of the multicast group to include in IPv4 prefixing format <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i> .</li> </ul>

## Command Default

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

## Command Modes

IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

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

**Caution**

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

```
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
<b>ping</b>	Checks host reachability and network connectivity on IP networks. For information, see <i>IP Addresses and Services Configuration Guide for Cisco NCS 6000 Series Routers</i> .



# maximum groups

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

**maximum groups** *number*

**no maximum groups**

## Syntax Description

<i>number</i>	Maximum number of groups accepted by a router. Range is 1 to 75000.
---------------	---

## Command Default

*number* : 50000

## Command Modes

IGMP configuration

IGMP VRF configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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:

**Related Commands**

Command	Description
<a href="#">maximum groups-per-interface, on page 17</a>	Configures the maximum number of groups for each interface accepted by a router.
<a href="#">show igmp summary, on page 41</a>	Displays group membership information for Internet Group Management Protocol (IGMP).

# maximum groups-per-interface

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

**maximum groups-per-interface** *number*

**no maximum groups-per-interface**

## Syntax Description

<i>number</i>	Maximum number of groups accepted by a router for each interface.
---------------	---

## Command Default

*number* : 20000

## Command Modes

IGMP configuration  
IGMP VRF configuration  
IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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



### Note

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

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

```
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
```

```
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
<a href="#">maximum groups, on page 15</a>	Configures the maximum number of groups used by Internet Group Management Protocol (IGMP) .
<a href="#">show igmp summary, on page 41</a>	Displays group membership information for Internet Group Management Protocol (IGMP).

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

**nsf lifetime** *seconds*

**no nsf lifetime**

#### Syntax Description

<i>seconds</i>	Maximum time for NSF mode. Range is 10 to 3600 seconds.
----------------	---

#### Command Default

*seconds* : 60

#### Command Modes

IGMP configuration  
IGMP VRF configuration

#### Command History

Release	Modification
Release 5.0.0	This command was introduced.

#### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

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

#### Task ID

Task ID	Operations
multicast	read, write

## Examples

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

```
RP/0/RP0/CPU0:router(config)# router igmp  
RP/0/RP0/CPU0:router(config-igmp)# nsf lifetime 120
```

## Related Commands

Command	Description
<b>nsf (multicast)</b>	Enables NSF capability for the multicast routing system.
<b>nsf lifetime (PIM)</b>	Configures the NSF timeout value for the PIM process.
<a href="#">show igmp nsf</a> , on page 39	Displays the state of NSF operation in IGMP.
<b>show mfib nsf</b>	Displays the state of NSF operation for the MFIB line cards.

# query-interval

To configure the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages, use the **query-interval** 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

<i>seconds</i>	Frequency used to send IGMP host-query messages. Range is 1 to 3600.
----------------	--

## Command Default

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

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

## Command Modes

IGMP VRF configuration  
IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

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

If the router hears no queries for the timeout period (controlled by the [query-timeout](#), on page 26 command), it becomes the querier.



**Note**

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

**Note**

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

```
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
<b>hello-interval (PIM)</b>	Configures the frequency of PIM hello messages.
<a href="#">query-timeout, on page 26</a>	Configures the timeout value before the router takes over as the querier for the interface.
<a href="#">show igmp groups, on page 33</a>	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

## query-max-response-time

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

**query-max-response-time** *seconds*

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

### Syntax Description

<i>seconds</i>	Maximum response time, in seconds, advertised in IGMP queries. Range is 1 to 12.
----------------	--

### Command Default

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

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

### Command Modes

IGMP VRF configuration

IGMP interface configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

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



#### Note

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

```
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
<b>hello-interval (PIM)</b>	Configures the frequency of PIM hello messages.
<a href="#">show igmp groups, on page 33</a>	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

# query-timeout

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

**query-timeout** *seconds*

**no query-timeout**

## Syntax Description

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

## Command Default

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

## Command Modes

IGMP VRF configuration  
IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **query timeout** command is not supported on Internet Group Management Protocol (IGMP) Version 1. By default, the router waits twice the query interval specified by the **query-interval** command, after which, if the router has heard no queries, it becomes the querier. By default, the query interval is 60 seconds, which means that the **query timeout** value defaults to 120 seconds.

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



### Note

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

```
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
<a href="#">query-interval, on page 22</a>	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.

# robustness-count

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

**robustness-count** *count*

**no robustness-count**

## Syntax Description

<i>count</i>	Value of the robustness count variable. Range is 2 to 10 packets.
--------------	---

## Command Default

Default is 2 packets.

## Command Modes

IGMP VRF configuration  
IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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) 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

<b>disable</b>	Turns off IGMP membership tracking.
<b>enable</b>	Turns on IGMP membership tracking.

## Command Default

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

## Command Modes

IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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



### Note

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

## Task ID

Task ID	Operations
mcast	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
<b>multicast routing</b>	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

XR Config

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** XR Config

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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	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
<b>interface all disable</b>	Disables IGMP membership tracking on all interfaces.
<b>multicast routing</b>	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 XR EXEC mode.

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

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<i>group-address</i>	(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.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Either a physical interface or a virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>not-active</b>	(Optional) Displays group joins that are not processed.
<b>summary</b>	(Optional) Displays the total number of (*, G) and (S, G) states in IGMP.
<b>detail</b>	(Optional) Displays detail information such as IGMP Version 3 source list, host, and router mode.
<b>explicit</b>	(Optional) Displays explicit tracking information.

## Command Default

No default behavior or values

## Command Modes

EXEC  
XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 2: show igmp groups Field Descriptions**

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

**Related Commands**

Command	Description
<a href="#">show igmp interface</a> , on page 35	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 XR EXEC mode.

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

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Either a physical interface or a virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>state-on</b>	(Optional) Displays all interfaces with IGMP enabled.
<b>state-off</b>	(Optional) Displays all interfaces with IGMP disabled.

## Command Default

No default behavior or values

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 3: 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 <b>address</b> command.
IGMP is enabled on interface	Indicates whether IGMP router functionality has been enabled on the interface.  <b>Note</b> 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 sends Protocol Independent Multicast (PIM) query messages, as specified with the <b>query-interval</b> 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.

Field	Description
IGMP querying router is 239.122.41.51 (this system)	Indicates the elected querier on the link.

**Related Commands**

Command	Description
<b>address</b>	Sets a primary or secondary IP address for an interface.
<a href="#">query-interval, on page 22</a>	Configures the frequency at which Cisco IOS XR software sends IGMP host-query messages.
<a href="#">router, on page 29</a>	Disables or enables 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 XR EXEC.

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

## Syntax Description

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

## Command Default

No default behavior or values

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

Non-Stop Forwarding Status

```
NSF
:      00:
:
```

This table describes the significant fields shown in the display.

**Table 4: 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
<b>nsf (multicast)</b>	Enables NSF capability for the multicast routing system.
<a href="#">, on page 20</a>	Configures the NSF timeout value for the IGMP or MLD process.
<b>nsf lifetime (PIM)</b>	Configures the NSF timeout value for the PIM process.
<b>show mfib nsf</b>	Displays the state of NSF operation for the MFIB line cards.
<b>show mrrib nsf</b>	Displays the state of NSF operation in the MRIB.
<b>show pim nsf</b>	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

XR EXEC

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

## Syntax Description

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

## Command Default

No default behavior or values

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

```
Bundle-Ether28.1          3          5
```

```
5
```

```
5
```

```
MgmtEth0/RP1/CPU0/0      0          5
```

```
3          5
```

```
5
```

```
5
```

```
5
```

```
3          5
```

```
/
/
/
```

```
5
```

```
GigabitEthernet0/
/5/
```

```
3          5
GigabitEthernet0/
/5/
```

```
5
```

```
/
/
/
```

```

          5
/6/
/
  3      5

/6/
/
  3      5

/6/
/
  3      5

```

This table describes the significant fields shown in the display.

**Table 5: show igmp summary Field Descriptions**

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

#### Related Commands

Command	Description
<a href="#">show igmp groups, on page 33</a>	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 XR EXEC

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

## Syntax Description

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

## Command Default

No default behavior or values

## Command Modes

EXEC  
XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## 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

XR EXEC

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

## Syntax Description

<b>vrf vrf-name</b>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
---------------------	---

## Command Default

No default behavior or values

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 the **show igmp traffic** command.

**Table 6: show igmp traffic Field Descriptions**

Field	Description
Valid IGMP Packet	Total number of valid protocol packets sent and received. Valid packet types include: <ul style="list-style-type: none"> <li>• Queries</li> <li>• Membership reports</li> <li>• Leaves</li> </ul>
Queries	Total number of query packets sent and received. IP Multicast routers send queries to determine the multicast reception state of neighboring interfaces.
Reports	Total number of membership report packets received. Membership reports indicate either the current multicast reception state of a neighboring interface or a change to that state.
Leaves	Total number of leaves received. A leave group packet indicates a neighboring interface no longer has multicast reception state for a particular group.
Mtrace packets	Total number of Mtrace packets sent and received. Mtrace traces the route from a receiver to a source using a particular multicast address.
DVMRP packets	Total number of Distance Vector Multicast Routing Protocol (DVMRP) packets sent and received. DVMRP is an Internet routing protocol that provides a mechanism for connectionless datagram delivery to a group of hosts across an internetwork. This protocol dynamically generates IP multicast delivery trees using Reverse Path Multicasting. Packet type 0x13 indicates a DVMRP packet.

Field	Description
PIM packets	Total number of sent and received Protocol Independent Multicast (PIM) packets.
Malformed Packets	Total number of malformed packets received. A malformed packet is a packet smaller than the smallest valid protocol packet.
Bad Checksums	Total number of packets received with a bad protocol header checksum.
Socket Errors	Total number of read and write failures on the protocol socket.
Bad Scope Errors	Total number of packets received with an invalid multicast scope.  <b>Note</b> 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 auxiliary 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.
Packets which couldn't be accessed	Total number of packets that could not be sent or received.  This might occur if: <ul style="list-style-type: none"> <li>• Packet buffer does not form a valid protocol packet.</li> <li>• IP header is not written to the packet.</li> <li>• Outgoing packet interface handle was not set.</li> <li>• Errors occurred calculating the protocol checksum.</li> </ul>
Other Packet Drops	Packets dropped for any other reason.

**Related Commands**

Command	Description
show pim traffic	Displays PIM traffic counter information.

## ssm map static

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, use the **ssm map static** 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

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

### Command Default

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

### Command Modes

IGMP VRF configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

PIM-SSM requires the use of IGMPv3 (IPv4) to determine local memberships. Under normal operating conditions, IGMP 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

<i>group-address</i>	IP address of the multicast group in IPv4 prefixing format: <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i> .</li> </ul>
<b>inc-mask</b> <i>mask</i>	(Optional) Specifies a mask for the increment range. This is an IP address expressed range in IPv4 format. This mask is used with the group address to generate subsequent group addresses: <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i> .</li> </ul> <p><b>Note</b> This mask is used with the group address to generate subsequent group addresses.</p>
<b>count</b> <i>cnt</i>	(Optional) Specifies a number of group addresses to generate using the increment mask. Range is 1 to 512.
<i>source address</i>	(Optional) Source address of the multicast group to include in IPv4 prefixing format: <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i> .</li> </ul>

## Command Default

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

## Command Modes

IGMP interface configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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) version for the router, use the **version** command in the appropriate configuration mode. To restore the default value, use the **no** form of this command.

**version** {1| 2| 3}

**no version**

### Syntax Description

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

### Command Default

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

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

### Command Modes

IGMP configuration  
IGMP VRF configuration  
IGMP interface configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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



**Note**

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

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

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

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

**Related Commands**

Command	Description
<a href="#">query-max-response-time, on page 24</a>	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.
<a href="#">query-timeout, on page 26</a>	Configures the timeout value before the router takes over as the querier for the interface.

## vrf (igmp)

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

**vrf** *vrf-name*

**no vrf** *vrf-name*

### Syntax Description

<i>vrf-name</i>	Name of the VRF instance.
-----------------	---------------------------

### Command Default

No default behavior or values

### Command Modes

IGMP configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

### Task ID

Task ID	Operations
multicast	read, write

### Examples

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

```
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 on

---

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

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the *Implementing Multicast Routing on* configuration module in *Multicast Configuration Guide for Cisco NCS 6000 Series Routers*.

- [cache-sa holdtime](#), page 59
- [cache-sa-state](#), page 61
- [clear msdp peer](#), page 63
- [clear msdp sa-cache](#), page 65
- [clear msdp stats](#), page 67
- [connect-source](#), page 69
- [default-peer](#) , page 71
- [description \(peer\)](#), page 73
- [maximum external-sa](#), page 75
- [maximum peer-external-sa](#), page 77
- [mesh-group \(peer\)](#), page 79
- [originator-id](#), page 81
- [password \(peer\)](#), page 83
- [peer \(MSDP\)](#), page 85
- [remote-as \(multicast\)](#), page 87
- [sa-filter](#), page 88
- [show msdp globals](#), page 90
- [show msdp peer](#), page 93

- [show msdp rpf](#) , page 96
- [show msdp sa-cache](#), page 98
- [show msdp statistics peer](#), page 103
- [show msdp summary](#), page 105
- [shutdown \(MSDP\)](#), page 107
- [ttl-threshold \(MSDP\)](#), page 109

## 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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">cache-sa-state</a> , on page 61	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

<b>list</b> <i>access-list-number</i>	Specifies an IP access list that defines which (S, G) pairs to cache.
<b>rp-list</b> <i>access-list-name</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show msdp sa-cache</a> , <a href="#">on page 98</a>	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

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>peer-address</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

clear msdp peer

Related Commands

Command	Description
<a href="#">peer (MSDP), on page 85</a>	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

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>group-address</i>	(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 5.0.0	This command was introduced,

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.



### 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
<a href="#">show msdp sa-cache</a> , on page 98	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

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

### Command Default

No default behavior or values

### Command Modes

EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

 clear msdp stats**Related Commands**

Command	Description
<a href="#">show msdp statistics peer</a> , <a href="#">on page 103</a>	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

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<i>ip-address</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">peer (MSDP), on page 85</a>	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

<i>peer-address</i>	IP address or hostname for the peer to which this description applies.
<i>text</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

description (peer)

**Related Commands**

Command	Description
<a href="#">peer (MSDP), on page 85</a>	Configures a Multicast Source Discovery Protocol (MSDP) peer.
<a href="#">show msdp peer, on page 93</a>	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

<i>entries</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 MSDP 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
<a href="#">maximum peer-external-sa</a> , <a href="#">on page 77</a>	Configures the maximum number of external Multicast Source Discovery Protocol (MSDP) Source-Active (SA) entries that can be learned from MSDP peers.
<a href="#">show msdp summary</a> , <a href="#">on page 105</a>	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

<i>entries</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">maximum external-sa, on page 75</a>	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.
<a href="#">show msdp summary, on page 105</a>	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

<i>name</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Mesh groups can be used to:

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

### Task ID

Task ID	Operations
multicast	read, write

## Examples

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

```
RP/0/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

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface. <b>Note</b> Use the <b>show interfaces</b> 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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<b>clear</b>	Specifies that an unencrypted password follows. The password must be a case-sensitive, clear-text unencrypted password.
<b>encrypted</b>	Specifies that an encrypted password follows. The password must be a case-sensitive, encrypted password.
<i>password</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

**Related Commands**

Command	Description
<a href="#">show mdp peer, on page 93</a>	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

<i>peer-address</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

### Task ID

Task ID	Operations
multicast	read, write

### Examples

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

```
RP/0/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
<a href="#">default-peer</a> , on page 71	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

<i>as-number</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 <b>sa-filter</b> 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 5.0.0	This command was introduced.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
------------------	---



Note	You can configure the <b>sa-filter</b> 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
<a href="#">peer (MSDP)</a> , <a href="#">on page 85</a>	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 XR EXEC.

**show msdp [ipv4] globals**

Syntax Description	<div> <div>ipv4</div> <div>(Optional) Specifies IPv4 address prefixes.</div> </div>
--------------------	---

Command Default	IPv4 addressing is the default.
-----------------	---------------------------------

Command Modes	XR EXEC
---------------	---------

Command History	<div> <div>Release</div> <div>Modification</div> </div>
	<div> <div>Release 5.0.0</div> <div>This command was introduced.</div> </div>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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	<div> <div>Task ID</div> <div>Operations</div> </div>
	<div> <div>multicast</div> <div>read</div> </div>

**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 allocated/free: 2/0
Total list items allocated/free: 9/1
Total source buffers allocated/free: 1/0
Total group buffers allocated/free: 1/0
Total RP buffers allocated/free: 2/0
TLV buffers allocated/free: 1/1

```

This table describes the significant fields shown in the display.

**Table 7: show msdp globals Field Descriptions**

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

Field	Description
Total RP buffers allocated/free	Number of internal RP buffers allocated and freed after allocation.
TLV buffers allocated/free	Number of internal time-to-live buffers allocated and freed after allocation.

**Related Commands**

Command	Description
<a href="#">show msdp peer, on page 93</a>	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
<a href="#">show msdp sa-cache, on page 98</a>	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 XR EXEC.

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

### Syntax Description

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

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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 8: show msdp peer Field Descriptions**

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



**Related Commands**

Command	Description
<a href="#">peer (MSDP), on page 85</a>	Configures a Multicast Source Discovery Protocol (MSDP) peer.
<a href="#">show msdp sa-cache, on page 98</a>	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 XR EXEC.

**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** XR EXEC

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 9: show msdp rpf Field Descriptions**

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

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

## Syntax Description

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>source-address</i>	(Optional) Source address or hostname of the source about which (S, G) information is displayed.
<i>group-address</i>	(Optional) Group address or name of the group about which (S, G) information is displayed.
<b>all</b>	(Optional) Displays all Source Active (SA) entries with PI (PIM Interested) flags.
<b>asnum</b> <i>as-number</i>	(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.
<b>peer</b> <i>peer-address</i>	(Optional) Displays peer entry information, including peer name and peer address.
<b>rpaddr</b> <i>rp-address</i>	(Optional) Displays SA entries that match the specified rendezvous point (RP) address.
<b>summary</b>	(Optional) Displays the count of all SA entries, RPs, sources, and groups.

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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, AS 20, 15:44:03/00:01:17
Learned from peer 10.10.2.2, RPF peer 10.10.2.2
SA's recvd 1049, Encapsulated data received: 0
grp flags: PI, src flags: E, EA, PI
```

This table describes the significant fields shown in the display.

**Table 10: show msdp sa-cache Field Descriptions**

Field	Description
(10.10.5.102, 239.1.1.1)	The first address (source) is sending to the second address (group).
RP 10.10.4.3	Rendezvous point (RP) address in the originating domain where the SA messages started.

Field	Description
MBGP/AS 20	RP is in autonomous system AS 20 according to the unicast RPF table: <ul style="list-style-type: none"> <li>• If Multiprotocol Border Gateway Protocol (MBGP) is not configured—RIB table 1.</li> <li>• If MBGP is configured—RIB table 2 or multicast table.</li> </ul>
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, AS 0, 06:32:18/expired
Learned from peer local, RPF peer local
SAs recvd 0, Encapsulated data received: 0 grp flags: PI, src flags:
This table describes the significant fields shown in the display.
```

**Table 11: show msdp sa-cache all Field Descriptions**

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

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

```
RP/0/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 12: show msdp sa-cache summary Field Descriptions**

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

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

```
RP/0/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, AS 200, 00:00:25/00:02:04
  Learned from peer 5.1.1.1, RPF peer 172.17.1.1
  SAs recvd 1, Encapsulated data received: 100
  grp flags: none, src flags: EA
(172.31.1.1, 239.1.1.2), RP 172.17.1.1, AS 200, 00:00:16/00:02:13
  Learned from peer 172.17.1.1, RPF peer 172.17.1.1
  SAs recvd 1, Encapsulated data received: 100
  grp flags: none, src flags: EA
```

**show msdp sa-cache**

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

**Related Commands**

Command	Description
<a href="#">cache-sa-state</a> , <a href="#">on page 61</a>	Controls cache source-active (SA) state on a router.
<a href="#">peer (MSDP)</a> , <a href="#">on page 85</a>	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 XR EXEC

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

### Syntax Description

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>peer-address</i>	(Optional) IP address or name of the MSDP peer.

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 13: show msdp statistic peer Field Descriptions**

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

## Related Commands

Command	Description
<a href="#">clear msdp stats</a> , on page 67	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

XR EXEC

.

**show msdp [ipv4] summary**

### Syntax Description

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
-------------	---

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/ Downtime	Reset Count	Peer Name	Active SA Cnt	Cfg.Max Ext.SAs	TLV recv/sent
10.1.1.1	0	NoIntf	00:10:07	0	?	0	0	0/0

This table describes the significant fields shown in the display.

**Table 14: show msdp summary Field Descriptions**

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

**Related Commands**

Command	Description
<a href="#">show msdp peer, on page 93</a>	Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
<a href="#">show msdp sa-cache, on page 98</a>	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 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

shutdown (MSDP)

**Related Commands**

Command	Description
<a href="#">show msdp peer, on page 93</a>	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

<i>ttl</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">peer (MSDP), on page 85</a>	Configures a Multicast Source Discovery Protocol (MSDP) peer.





# Multicast Routing and Forwarding Commands on

---

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

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 *Multicast Configuration Guide for Cisco NCS 6000 Series Routers*.

- [accounting per-prefix, page 113](#)
- [accounting per-prefix forward-only, page 115](#)
- [address-family \(multicast\), page 117](#)
- [boundary, page 120](#)
- [clear mfib counter, page 121](#)
- [clear mfib database, page 123](#)
- [clear mfib hardware adjacency-counters, page 124](#)
- [disable \(multicast\), page 125](#)
- [enable \(multicast\), page 127](#)
- [forwarding-latency, page 129](#)
- [interface \(multicast\), page 131](#)
- [interface all enable, page 133](#)
- [interface-inheritance disable, page 135](#)
- [log-traps, page 137](#)
- [maximum disable, page 138](#)
- [mdt data, page 139](#)
- [mdt default, page 141](#)
- [mdt mtu, page 143](#)
- [mdt source, page 145](#)

- [mhost default-interface](#), page 147
- [multicast-routing](#), page 149
- [nsf \(multicast\)](#) , page 151
- [oom-handling](#), page 153
- [rate-per-route](#), page 155
- [show mfib connections](#), page 156
- [show mfib counter](#), page 158
- [show mfib encap-info](#) , page 160
- [show mfib hardware route accept-bitmap](#), page 162
- [show mfib hardware route olist](#), page 164
- [show mhost default-interface](#), page 166
- [show mhost groups](#) , page 168
- [show mrrib client](#), page 170
- [show mrrib nsf](#), page 173
- [show mrrib route](#), page 175
- [show mrrib route-collapse](#), page 177
- [show mrrib route outgoing-interface](#), page 179
- [show mrrib table-info](#), page 181
- [show mrrib tlc](#), page 183
- [ttl-threshold \(multicast\)](#), page 185
- [vrf \(multicast\)](#), page 187

# accounting per-prefix

To enable accounting for multicast routing, use the **accounting per-prefix** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**accounting per-prefix**

**no accounting per-prefix**

**Syntax Description** This command has no keywords or arguments.

**Command Default** This feature is disabled by default.

**Command Modes**

- Multicast routing configuration
- Multicast routing address family IPv4 configuration
- Multicast VRF configuration

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

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 the **accounting per-prefix** command is .

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
<a href="#">show mfib route</a>	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 113, 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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.



#### 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 recommend 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

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 113](#) 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
<a href="#">accounting per-prefix, on page 113</a>	Enables accounting for multicast routing.

## 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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	Specifies IPv4 address prefixes.
<b>ipv6</b>	Specifies IPv6 address prefixes.

### Command Default

No default behavior or values

### Command Modes

Multicast routing configuration  
Multicast VRF configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **address-family** command either from multicast routing configuration mode or from multicast VRF configuration submode 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 149](#) 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 135](#) 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 andIPv6 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
<b>alias</b>	Creates a command alias.
<a href="#">interface all enable, on page 133</a>	Enables multicast routing and forwarding on all new and existing interfaces.
<b>interface all disable</b>	Disables PIM processing on all new and existing interfaces.
<a href="#">interface-inheritance disable, on page 135</a>	Separates the disabling of multicast routing and forwarding.
<a href="#">interface (multicast), on page 131</a>	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

<i>access-list</i>	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 5.0.0	This command was introduced.

## 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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>group-address</i>	(Optional) IP address of the multicast group.
<i>source-address</i>	(Optional) IP address of the source of the multicast route.
<b>location</b> <i>node-id</i>	(Optional) Clears route packet counters from the designated node.
<b>all</b>	The <b>all</b> keyword clears route packet counters on all nodes

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.



### 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

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>location</b> <i>node-id</i>	(Optional) Clears global resource counters from the designated node.
<b>all</b>	The <b>all</b> keyword clears all global resource counters.

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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 adjacency-counters

To clear the platform-specific information related to resource counters for the Multicast Forwarding Information Base, use the **clear mfib hardware adjacency-counters** command in the appropriate mode.

**clear mfib** [**vrf** *vrf-name*] [**ipv4**] **hardware adjacency-counters** [**rx**|**tx**] [**location** {*node-id*|**all**}]

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>rx</b>	Clears adjacency counters for packets received.
<b>tx</b>	Clears adjacency counters for packets sent.
<b>location</b> <i>node-id</i>	(Optional) Clears adjacency counters from the designated node.

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## Task ID

Task ID	Operations
multicast	read, write, execute

## Examples

The following example shows how to clear all adjacency counters:

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

## 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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">enable (multicast), on page 127</a>	Enables multicast routing and forwarding on an interface.
<a href="#">interface all enable, on page 133</a>	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

Release	Modification
Release 5.0.0	This command was introduced.

**Command History**

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">disable (multicast)</a> , on page 125	Disables multicast routing and forwarding on an interface.
<a href="#">interface all enable</a> , on page 133	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

<b>delay milliseconds</b>	(Optional) Specifies the delay time in milliseconds. 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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

## Command Default

No default behavior or values

## Command Modes

Multicast routing configuration  
IPv4 or multicast routing configuration  
Multicast VRF configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">disable (multicast), on page 125</a>	Disables multicast routing and forwarding on an interface.
<a href="#">enable (multicast), on page 127</a>	Enables multicast routing and forwarding on an interface.
<a href="#">interface all enable, on page 133</a>	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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">disable (multicast), on page 125</a>	Disables multicast routing and forwarding on an interface.
<a href="#">enable (multicast), on page 127</a>	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 submode. To restore the default functionality, use the **no** form of the command.

**interface-inheritance disable**

**no interface-inheritance disable**

## Syntax Description

This command has no keywords or arguments.

## Command Default

This feature is not enabled by default.

## Command Modes

Multicast routing configuration

Address- family IPv4 configuration

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use of the **interface-inheritance disable** command together with the **interface type interface-path-id** or **interface all enable** command under multicast routing address-family IPv4 submode separates PIM and IGMP routing functionality from multicast forwarding on specified interfaces. You can nonetheless enable multicast routing functionality explicitly under PIM or IGMP routing configuration mode for individual interfaces.



### Note

Although you can explicitly configure multicast routing functionality on individual interfaces, you cannot explicitly disable the functionality. You can only disable the functionality on all interfaces.

Used from the address-family ipv4 configuration submode, it prevents IGMP and PIM from inheriting the multicast-routing interface configuration.

## Task ID

Task ID	Operations
multicast	read, write

## Examples

The following configuration disables PIM and IGMP routing functionality on all the interfaces using the **interface-inheritance disable** command, but multicast forwarding is still enabled on all the interfaces in the example, based on use of the keywords **interface all enable**.

PIM is enabled on *Loopback 0* based on its explicit configuration ( **interface Loopback0 enable** ) under router pim configuration mode.

IGMP protocol is enabled on GigabitEthernet0/6/0/3, because it too has been configured explicitly under router igmp configuration mode ( **interface GigabitEthernet0/6/0/3 router enable** ):

```
RP/0/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 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 address family IPv4 configuration  
Multicast VRF configuration

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 address family IPv4 configuration  
Multicast VRF configuration

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **maximum disable** command to override the default software limit on the number of multicast routes.

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

<i>mdt-group-address</i>	IP address of the MDT group.
<i>/ mask</i>	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.
<b>threshold</b> <i>threshold</i>	Specifies the traffic rate threshold to trigger data MDT. Range is 1 to 4294967295.
<i>acl-name</i>	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

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

### Related Commands

Command	Description
<a href="#">mdt default, on page 141</a>	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).
<a href="#">mdt mtu, on page 143</a>	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).
<a href="#">mdt source, on page 145</a>	Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.

## 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

<i>mdt-default-group-address</i>	IP address of the MDT default group entered in <i>A.B.C.D.</i> format.
<b>ipv4</b>	Specifies IPv4-encapsulated MDT.
<i>mdt-default-address</i>	MDT IPv4 default address entered in <i>A.B.C.D.</i> 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

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Although within the multicast VRF configuration submenu, 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
<a href="#">mdt data, on page 139</a>	Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).
<a href="#">mdt mtu, on page 143</a>	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).
<a href="#">mdt source, on page 145</a>	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

<i>value</i>	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

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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
<a href="#">mdt data, on page 139</a>	Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).
<a href="#">mdt default, on page 141</a>	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).
<a href="#">mdt source, on page 145</a>	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

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">mdt data, on page 139</a>	Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).
<a href="#">mdt default, on page 141</a>	Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).
<a href="#">mdt mtu, on page 143</a>	Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).

## mhost default-interface

To configure the default interface for IP multicast transmission and reception to and from the host stack, use the **mhost default-interface** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**mhost {ipv4| ipv6} default-interface** *type interface-path-id*

**no mhost {ipv4| ipv6} default-interface** *type interface-path-id*

### Syntax Description

<b>ipv4</b>	Specifies IPv4 address prefixes.
<b>ipv6</b>	Specifies IPv6 address prefixes.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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 Multicast Host (MHost) default interface is configured, an arbitrary interface is selected as the active MHost default.

If multicast routing feature is enabled, a multicast-enabled interface is always selected as the MHost default interface.

### Command Modes

Global configuration  
XR Config  
Global VRF configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **mhost default-interface** command configures the interface that the automatic route processing (Auto-RP), ping, and mtrace applications use for multicast transmissions, and the interface to which multicast groups are joined for reception.

and mtrace may use the MHost default interface to process multicast messaging. When IP multicast routing is enabled, packets sent to the MHost default interface are switched on other interfaces with a matching forwarding state. In addition, an arbitrary interface may be chosen to be the active MHost default interface if the configured interface is not operational. If no MHost default interface is configured with this command, an arbitrary interface is selected as the active MHost default.

**Note**

- The MHost default interface must be configured explicitly (preferably use a loopback interface).
- If the MHost default interface is not configured explicitly, then the router picks an interface.
- If the router picked multicast interface happens to be an ASBR link (on an ASBR router) and if that interface is configured with multicast boundary, then it may not work as intended because there is an IC (Internal Copy) flag on the interface and it has to accept all multicast packets on the interface.

**Task ID**

Task ID	Operations
multicast	read, write

**Examples**

The following example shows how to configure Loopback interface 1 as the default interface:

```
RP/0/RP0/CPU0:router(config)# mhost ipv4 default-interface loopback 1
```

**Related Commands**

Command	Description
<a href="#">show mhost default-interface</a> , on page 166	Displays the active default interface for the Multicast Host (MHost) process.

# multicast-routing

To enter multicast routing configuration mode, use the **multicast-routing** command in XR Config 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** XR Config

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
	<a href="#">accounting per-prefix, on page 113</a>	Enables per-prefix counters only in hardware.
	<b>alias</b>	Creates a command alias.

Command	Description
<a href="#">interface (multicast), on page 131</a>	Configures multicast interface properties.
<a href="#">interface all enable, on page 133</a>	Enables multicast routing and forwarding on all new and existing interfaces.



## 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

<b>lifetime</b> <i>seconds</i>	(Optional) Specifies the maximum time (in seconds) for NSF mode. Range is 30 to 3600.
--------------------------------	---

### Command Default

This command is disabled by default.

### Command Modes

Multicast routing configuration  
Multicast routing address family ipv4 configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 (MFW) 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
	Configures the maximum time for the NSF timeout value under IGMP.
<b>nsf lifetime (PIM)</b>	Configures the NSF timeout value for the PIM process.
<b>show igmp nsf</b>	Displays the state of NSF operation in IGMP.
<a href="#">show mfib nsf</a>	Displays the state of NSF operation for the MFIB line cards.
<a href="#">show mrrib nsf</a> , on page 173	Displays the state of NSF operation in the MRIB.
<b>show pim nsf</b>	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 address family ipv4 configuration

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<b>show pim topology</b>	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 address family ipv4 configuration  
Multicast VRF configuration

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

Command	Description
<a href="#">show mfib route</a>	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 .

<b>Syntax Description</b>	<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
	<b>location</b> <i>node-id</i>	(Optional) Specifies MFIB connections associated with an interface of the designated node.

**Command Default** IPv4 addressing is the default.

**Command Modes** XR EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show mfib connections** command to display a list of servers connected to the MFIB and the status of the connections.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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
<a href="#">show mfib interface</a>	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
<a href="#">show mfib route</a>	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.

<b>Syntax Description</b>	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
	<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
	<b>location</b> <i>node-id</i>	(Optional) Specifies MFIB counter statistics associated with an interface of the designated node.

**Command Default** IPv4 addressing is the default.

**Command Modes** XR EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mfib counter** command displays packet drop statistics for packets that cannot be accounted for under route counters.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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 15: 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
<a href="#">show mfib interface</a>	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
<a href="#">show mfib route</a>	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.

<b>Syntax Description</b>	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
	<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
	<b>ipv6</b>	(Optional) Specifies IPv6 address prefixes.
	<b>location</b> <i>node-id</i>	(Optional) Specifies MFIB connections associated with an interface of the designated node.

**Command Default** IPv4 addressing is the default.

**Command Modes**  
EXEC  
XR EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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
<a href="#">show mfib interface</a>	Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.
<a href="#">show mfib route</a>	Displays route entries in the Multicast Forwarding Information Base (MFIB).

## 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 XR 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

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
	(Optional) Displays shared tree entry.
<i>source-address</i>	(Optional) IP address or hostname of the multicast route source:
<i>group-address</i>	(Optional) IP address or hostname of the multicast group.
<i>/ prefix-length</i>	(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.
<b>location</b> <i>node-id</i>	Specifies an MFIB-designated node.

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.



#### 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

**Related Commands**

Command	Description
<a href="#">show mfib interface</a>	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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
	(Optional) Displays shared tree entries.
<i>source-address</i>	(Optional) IP address or hostname of the multicast route source.
<i>group-address</i>	(Optional) IP address or hostname of the multicast group.
<i>/ prefix-length</i>	(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.
<b>location</b> <i>node-id</i>	Specifies an MFIB-designated node.

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show mfib route</a>	Displays route entries in the Multicast Forwarding Information Base (MFIB).

# show mhost default-interface

To display the active default interface for the Multicast Host (MHost) process, use the **show mhost default-interface** command in the appropriate mode .

<b>Syntax Description</b>	<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
	<b>ipv6</b>	(Optional) Specifies IPv6 address prefixes.

**Command Default** IPv4 addressing is the default.

**Command Modes** XR EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.

**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 **show mhost default-interface** command is used to show both the configured and active MHost default interfaces. The configured interface is the one specified by the **mhost default-interface** command; otherwise, the configured interface is displayed as none.

The active interface is the one currently being used as the default. The active interface may differ from the one configured when multicast routing is enabled and the configured interface is not operational. This command is useful when applications such as ping, or MTrace are not functioning as expected.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	network	read

**Examples**

The following is sample output for the **show mhost default-interface** command that shows that loopback interface 0 was configured as the MHost default interface, and it is the active default interface:

```
RP/0/RP0/CPU0:router# show mhost default-interface

mhost configured default interface is 'Loopback0'
mhost active default interface is 'Loopback0'
```



**Related Commands**

Command	Description
<a href="#">mhost default-interface, on page 147</a>	Configures the default interface for IP multicast transmission and reception to and from the host stack.

# show mhost groups

To display various multicast groups joined directly on the interface, use the **show mhost groups** command in the appropriate mode .

**show mhost** [**ipv4**] **groups** *type interface-path-id* [**location** *node-id*]

## Syntax Description

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>ipv6</b>	(Optional) Specifies IPv6 address prefixes.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>location</b> <i>node-id</i>	(Optional) Specifies a designated node.

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mhost groups** command is used to display the groups joined by applications and verifies that the MHost application is functioning properly.

## Task ID

Task ID	Operations
network	read

## Examples

The following is sample output from the **show mhost groups** command that shows the MHost groups 239.1.1.1, 224.0.0.22, 224.0.0.2, 224.0.0.1, 224.0.0.13, and 224.0.1.40 have joined on loopback 0 interface:

```
RP/0/RP0/CPU0:router# show mhost groups loopback 0

Loopback 0
239.1.1.1 : includes 1, excludes 0, mode INCLUDE
33.3.3.3 : includes 1, excludes 0, active in INCLUDE filter
224.0.0.22 : includes 0, excludes 1, mode EXCLUDE
<no source filter>
224.0.0.2 : includes 0, excludes 1, mode EXCLUDE
<no source filter>
224.0.0.1 : includes 0, excludes 1, mode EXCLUDE
<no source filter>
224.0.0.13 : includes 0, excludes 1, mode EXCLUDE
<no source filter>
224.0.1.40 : includes 0, excludes 2, mode EXCLUDE
<no source filter>
```

This table describes the significant fields shown in the display.

**Table 16: show mhost groups Field Descriptions**

Field	Description
includes	Number of source addresses in the include list.
excludes	Number of source addresses in the exclude list.
mode	Multicast socket filter mode: include or exclude.
33.3.3.3	Source address list to be included or excluded based on the multicast filter mode.

## Related Commands

Command	Description
<a href="#">show mfib hardware route accept-bitmap</a> , on page 162	Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.
<a href="#">show mfib hardware route olist</a> , on page 164	Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.
<a href="#">show mfib hardware route summary</a>	Displays summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry.
<a href="#">show mfib route</a>	Displays route entries in the Multicast Forwarding Information Base (MFIB).

## 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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>ipv6</b>	(Optional) Specifies IPv6 address prefixes.
<b>filter</b>	(Optional) Displays route and interface level flag changes that various MRIB clients have registered and shows what flags are owned by the MRIB clients.
<i>client-name</i>	(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

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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 17: 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 0.0.0.0/0 interfaces: 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
<a href="#">show mfib nsf</a>	Displays the state of a nonstop forwarding (NSF) operation for the Multicast Forwarding Information Base (MFIB) line cards.
<a href="#">show mfib route</a>	Displays route entries in the Multicast Forwarding Information Base (MFIB).
<a href="#">show mrib nsf, on page 173</a>	Displays the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB).

# 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.
------	---

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 18: 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
<a href="#">nsf (multicast)</a> , on page 151	Configures the NSF capability for the multicast routing system.
	Configures the maximum time for the NSF timeout value under IGMP .
<b>nsf lifetime (PIM)</b>	Configures the NSF timeout value for the PIM process.
<b>show igmp nsf</b>	Displays the state of NSF operation in IGMP.
<a href="#">show mfib nsf</a>	Displays the state of NSF operation in the MFIB line cards.
<b>show pim nsf</b>	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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>*</b>	(Optional) Displays shared tree entries.
<i>source-address</i>	(Optional) Source IP address or hostname of the MRIB route. Format is: <i>A.B.C.D</i> or <i>X:X::X</i> .
<i>group-address</i>	(Optional) Group IP address or hostname of the MRIB route. F ormat is: <i>A.B.C.D</i> or <i>X:X::X</i> .
<i>/prefix-length</i>	(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: <i>A.B.C.D</i> or <i>X:X::X</i> .
<b>outgoing-interface</b>	(Optional) Displays the outgoing-interface information.
<b>summary</b>	(Optional) Displays a summary of the routing database.
<b>detail</b>	(Optional) Displays the routing database with the platform data.

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release 5.0.0	This command was introduced.
---------------	------------------------------

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 158](#) command displays global counters independent of the routes.

**Task ID**

Task ID	Operations
multicast	read

**Related Commands**

Command	Description
	Configures the maximum time for the NSF timeout value on the IGMP.
<a href="#">show mfib counter, on page 158</a>	Displays MFIB counter statistics for packets that have dropped.
<a href="#">show mrib route-collapse, on page 177</a>	Displays the contents of the MRIB route collapse database.
<a href="#">show mfib route</a>	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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>core-tree</i>	(Optional) IPv4 Multicast Distribution Tree (MDT) group address.

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## 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
<a href="#">show mrrib route</a> , <a href="#">on page 175</a>	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

<i>*</i>	(Optional) Displays shared tree entries.
<i>A.B.C.D</i>	(Optional) Source IP address or hostname of the MRIB route. Format is: <i>A.B.C.D</i>
<i>A.B.C.D</i>	(Optional) Group IP address or hostname of the MRIB route and the prefix length.
<i>/prefix-length</i>	(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: <i>A.B.C.D</i>

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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
<a href="#">show mrib route</a> , on page 175	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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## 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 19: 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
<a href="#">show mrib tlc, on page 183</a>	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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## 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 20: 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.

## 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

<i>ttl</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<b>ttl-threshold (MSDP)</b>	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

<i>vrf-name</i>	Name of the VRF instance. The following names cannot be used: all, default, and global.
<b>ipv4</b>	(Optional) Configures IPv4 address prefixes.

### Command Default

No default behavior or values.

### Command Modes

Multicast routing configuration

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">boundary, on page 120</a>	Configures a boundary to keep multicast packets from being forwarded.
<a href="#">accounting per-prefix, on page 113</a>	Enables per-prefix counters only in hardware.
<a href="#">interface (multicast), on page 131</a>	Configures multicast interface properties.
<a href="#">log-traps, on page 137</a>	Enables logging of trap events.
<a href="#">multipath</a>	Enables Protocol Independent Multicast (PIM) to divide the multicast load among several equal-cost paths.
<a href="#">rate-per-route, on page 155</a>	Enables individual (source, group [S, G]) rate calculations.
<b>ssm</b>	Defines the Protocol Independent Multicast (PIM)-Source Specific Multicast (SSM) range of IP multicast addresses.
<a href="#">static-rpf</a>	Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.



## Multicast PIM Commands on

This chapter describes the commands used to configure and monitor Protocol Independent Multicast (PIM). For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Multicast Configuration Guide for Cisco NCS 6000 Series Routers*.

- [accept-register, page 191](#)
- [auto-rp candidate-rp, page 193](#)
- [bsr-border, page 196](#)
- [bsr candidate-bsr, page 198](#)
- [bsr candidate-rp, page 200](#)
- [clear pim counters, page 202](#)
- [clear pim topology, page 205](#)
- [dr-priority, page 207](#)
- [global maximum, page 209](#)
- [hello-interval \(PIM\), page 211](#)
- [interface \(PIM\), page 213](#)
- [join-prune-interval, page 215](#)
- [maximum register-states, page 217](#)
- [maximum route-interfaces, page 219](#)
- [maximum routes, page 221](#)
- [mofrr, page 223](#)
- [neighbor-check-on-recv enable, page 225](#)
- [neighbor-check-on-send enable, page 226](#)
- [neighbor-filter, page 227](#)
- [nsf lifetime \(PIM\), page 228](#)
- [old-register-checksum, page 230](#)

- [router pim](#), page 232
- [rp-address](#), page 234
- [rpf topology route-policy](#), page 236
- [rpf-vector](#) , page 238
- [rp-static-deny](#) , page 239
- [show auto-rp candidate-rp](#), page 240
- [show pim context](#), page 242
- [show pim context table](#), page 245
- [show pim group-map](#), page 247
- [show pim interface](#), page 249
- [show pim join-prune statistic](#), page 252
- [show pim mstatic](#), page 254
- [show pim neighbor](#), page 256
- [show pim nsf](#), page 259
- [show pim range-list](#), page 261
- [show pim summary](#), page 263
- [show pim topology](#), page 265
- [show pim topology detail](#), page 271
- [show pim topology entry-flag](#), page 274
- [show pim topology interface-flag](#), page 277
- [show pim topology summary](#), page 280
- [show pim traffic](#), page 282
- [show pim tunnel info](#), page 285
- [spt-threshold infinity](#), page 287
- [ssm](#), page 288



# 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	<i>access-list-name</i>	Access list number or name.
--------------------	-------------------------	-----------------------------

Command Default	No default behavior or values
-----------------	-------------------------------

Command Modes	PIM configuration
---------------	-------------------

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
------------------	---

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

### Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>scope</b> <i>ttl-value</i>	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.
<b>group-list</b> <i>access-list-name</i>	(Optional) Specifies an access list that describes the group ranges for which this router is the rendezvous point.
<b>interval</b> <i>seconds</i>	(Optional) Specifies the time between rendezvous point announcements. Range is 1 to 600.

### 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 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

# 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 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<i>ip-address</i>	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.
<b>hash-mask-len</b> <i>length</i>	(Optional) Specifies the length of a mask that is to be used in the hash function. <ul style="list-style-type: none"><li>• 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.</li><li>• For IPv4 addresses, we recommend a value of 30. The range is 0 to 32.</li><li>• For IPv6 addresses, we recommend a value of 126. The range is 0 to 128.</li></ul>
<b>priority</b> <i>value</i>	(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

Command Modes

PIM configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

# 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.

Command Default value : 1

Command Modes PIM configuration

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">bsr candidate-bsr, on page 198</a>	Configures the router to announce its candidacy as a bootstrap router (BSR).

# clear pim counters

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

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>ipv6</b>	(Optional) Specifies IPv6 address prefixes.

## Command Default

No default behavior or values

## Command Modes

EXEC  
XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Valid PIM Packets  Received          Sent
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 21: 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 <b>clear pim counters</b> 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.

```
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
<a href="#">show pim traffic, on page 282</a>	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.

Syntax Description	
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>ip-address-name</i>	(Optional) Can be either one of the following: <ul style="list-style-type: none"> <li>• Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the <b>domain IPv4</b> or <b>domain IPv6 host</b> command.</li> <li>• IP address of the multicast group, in IPv4 or IPv6 format according to the specified address family.</li> </ul>
<b>reset</b>	(Optional) Deletes all entries from the topology table and resets the MRIB connection.

**Command Default** No default behavior or values

**Command Modes** EXEC  
XR EXEC

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<i>value</i>	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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

# 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

<b>register states</b>	(Optional) Specifies the PIM source register states for all VRFs. Range is 0 to 75000.
<b>route-interfaces</b>	(Optional) Specifies the total number of PIM interfaces on routes for all VRFs. Range is 1 to 600000.
<b>routes</b>	(Optional) Specifies the PIM routes for all VRFs. Range is 1 to 200000.

## Command Default

No default value.

## Command Modes

PIM configuration

## Command History

Release	Modification
Release 3.9.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

## 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
```

## 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

<i>seconds</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">dr-priority, on page 207</a>	Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.
<a href="#">show pim neighbor, on page 256</a>	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

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface. <b>Note</b> Use the <b>show interfaces</b> 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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">dr-priority, on page 207</a>	Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.
<a href="#">hello-interval (PIM), on page 211</a>	Configures the frequency of Protocol Independent Multicast (PIM) hello messages.
<a href="#">join-prune-interval, on page 215</a>	Configures the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic.



# join-prune-interval

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

**join-prune-interval** *seconds*

**no join-prune-interval**

## Syntax Description

<i>seconds</i>	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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.



### 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
```

## 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

<i>number</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show pim summary, on page 263</a>	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

<i>number</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show pim summary, on page 263</a>	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	<i>number</i>	Maximum number of PIM routes. Range is 1 to 200000.
--------------------	---------------	---

Command Default	<i>number</i> : 100000
-----------------	------------------------

Command Modes	PIM configuration
---------------	-------------------

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

Usage Guidelines	<p>To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.</p> <p>The <b>maximum routes</b> command is used to set an upper limit for PIM routes. When the limit is reached, PIM discontinues route creation for its topology table.</p>
------------------	--

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
<a href="#">show pim summary, on page 263</a>	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,

**mofrr rib** *acl\_name*

**no rib** *acl\_name*

## Syntax Description

<i>acl_name</i>	Specifies the flows (S, G) s to be enabled by MoFRR.
-----------------	--

## Command Default

MoFRR is not enabled by default.

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

## Command Modes

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.



### 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
<b>show mfib counter</b>	Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.
<b>show mfib route</b>	Displays route entries in the MFIB.
<b>show mrrib route</b>	Displays all entries in the Multicast Routing Information Base (MRIB).
<a href="#">show pim rpf hash</a>	Displays MoFRR hashing information for Routing Information Base (RIB) lookups used to predict RPF next-hop paths for routing tables in PIM.
<a href="#">show pim rpf summary</a>	Displays summary information about the interaction of PIM with the RIB.
<a href="#">show pim topology detail, on page 271</a>	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.
<a href="#">show pim topology, on page 265</a>	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

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
```

Command	Description
<a href="#">neighbor-check-on-send enable</a> , on page 226	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 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
	<a href="#">neighbor-check-on-recv enable</a> , on page 225	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

<i>access-list</i>	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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<i>seconds</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<b>nsf (multicast)</b>	Turns on NSF capability for the multicast routing system.
<b>show igmp nsf</b>	Displays the state of NSF operation in IGMP.
<b>show mfib nsf</b>	Displays the state of NSF operation for the MFIB line cards.
<b>show mrrib nsf</b>	Displays the state of NSF operation in the MRIB.
<a href="#">show pim nsf, on page 259</a>	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

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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	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 XR Config 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

XR Config

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

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

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

### Task ID

Task ID	Operations
multicast	read, write

### Examples

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

```
RP/0/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
```

### Related Commands

Command	Description
<b>ipv4 access-list</b>	Defines a standard IP access list. For more information, see <i>IP Addresses and Services Configuration Guide for Cisco NCS 6000 Series Routers</i>

# 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 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For information about routing policy commands and how to create a routing policy, see *Routing Command Reference for Cisco NCS 6000 Series Routers* and *Routing Configuration Guide for Cisco NCS 6000 Series Routers*.

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

Task ID	Task ID	Operations
	multicast	read, write

## Examples

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

```
RP/0/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-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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<i>access-list</i>	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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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
<b>ipv4 access-list</b>	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 XR EXEC

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

Syntax Description	ipv4 (Optional) Specifies IPv4 address prefixes.
--------------------	--

Command Default	IPv4 addressing is the default.
-----------------	---------------------------------

Command Modes	EXEC XR EXEC
---------------	-----------------

Command History	Release Modification
Release 5.0.0	This command was introduced.

Usage Guidelines	<p>To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.</p> <p>The <b>show auto-rp candidate-rp</b> command displays all the candidate rendezvous points configured on this router.</p> <p>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.</p>
------------------	--

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 22: 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.

# show pim context

To show the reverse path forwarding (RPF) table information configured for a VRF context, use the **show pim context** command in XR EXEC

**show pim** [*vrf vrf-name*] [*ipv4| ipv6*] context

Syntax Description	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
	<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

**Command Default** IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes** XR EXEC

Command History	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID	<b>Task ID</b>	<b>Operations</b>
	multicast	read

**Examples** The following example illustrates output from use of the **show pim context** command:

```
RP/0/RP0/CPU0:router# show pim context
```

The following table gives the field descriptions for the **show pim context** command output:

**Table 23: show pim context Field Descriptions**

Field	Description
VRF ID	VPN routing and forwarding instance identification.
Table ID	Identification of unicast default table as of VRF context activation.
Remote Table ID	Identifies the table ID of the opposite address family. For example, the remote table ID for the VRF context of the
MDT Default Group	Identifies the multicast distribution tree (MDT) group configured as the default for use by the VRF.
MDT handle	Identifies the handle for multicast packets to be passed through the MDT interface.
Context Active	Identifies whether or not the VRF context was activated.
ITAL Active	Identifies whether or not the VRF is registered with ITAL. If it is, this signifies that the VRF is configured globally.
Routing Enabled	Identifies whether or not PIM is enabled in the VRF.
Registered with MRIB	Identifies whether or not the VRF is registered with Multicast Routing Information Base (MRIB).
Not owner of MDT interface	Identifies a process as not being the owner of the MDT interface. The owner is either the PIM or the PIM IPv6 process.
Owner of MDT interface	Identifies the owner of the MDT interface. The owner is either the PIM or the PIM IPv6 process.
Raw socket req:	Raw socket operations requested.
act:	Action: Indicates whether or not the operations were performed.
T; F	True; False
LPTS filter req	Identifies whether or not the VRF was requested to be added to the socket.
UDP socket req	Identifies whether or not a UDP socket was requested.

Field	Description
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 there is no neighbor filter, the output reads: "-".

## show pim context table

To display a summary list of all tables currently configured for a VRF context, use the **show pim context table** command in XR EXEC.

**show pim [vrf vrf-name] [ipv4|ipv6] context table**

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

### Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

### Command Modes

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### 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/ /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

show pim context table

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 24: show pim ipv4 context table Field Descriptions

Field	Description
Table	Context table name.
Table ID	RSI table ID for the table.
Status	<p>Identifies whether or not the context table is active or inactive.</p> <p>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.</p>



# show pim group-map

To display group-to-PIM mode mapping, use the **show pim group-map** command in XR EXEC mode.

**show pim** [**vrf** *vrf-name*] [**ipv4**|**ipv6**] **group-map** [ *ip-address-name* ] [**info-source**]

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>info-source</b>	(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

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 25: 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 <i>IP Addresses and Services Configuration Guide for Cisco NCS 6000 Series Routers</i>
<a href="#">rp-address, on page 234</a>	Configures the address of a PIM rendezvous point for a particular group.
<a href="#">show pim range-list, on page 261</a>	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 XR EXEC mode.

**show pim** [**vrf** *vrf-name*] [**ipv4**|**ipv6**] **interface** [*type interface-path-id*] **state-on**|**state-off**] [**detail**]

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>state-on</b>	(Optional) Displays only interfaces from which PIM is enabled and active.
<b>state-off</b>	(Optional) Displays only interfaces from which PIM is disabled or inactive.
<b>detail</b>	(Optional) Displays detailed address information.

## Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 Count	Hello Intvl	DR Prior	DR
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 26: 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 <b>ip pim hello-interval</b> 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
<a href="#">show pim neighbor</a> , on page 256	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.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 27: show pim join-prune statistics Field Descriptions**

Field	Description
Interface	Interface from which statistics were collected.
MTU	Maximum transmission unit (MTU) in bytes for the interface.
Transmitted	Number of join and prune states aggregated into transmitted messages in the last 1000/10000/50000 transmitted join and prune messages.
Received	Number of join and prune states aggregated into received messages in the last 1000/10000/50000 received join and prune messages.

# show pim mstatic

To display multicast static routing information, use the **show pim mstatic** command in XR EXEC mode.

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

Syntax Description	ipv4 (Optional) Specifies IPv4 address prefixes.
--------------------	--

Command Default	IPv4 addressing is the default.
-----------------	---------------------------------

Command Modes	XR EXEC
---------------	---------

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 28: 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
<b>static-rpf</b>	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 XR EXEC mode.

**show pim** [*vrf vrf-name*] [*ipv4| ipv6*] **neighbor** [*type interface-path-id*] [*count| detail*]

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>count</b>	(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.
<b>detail</b>	(Optional) Displays detailed information.

## Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**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 29: 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.

Field	Description
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.
Nbr count	Number of PIM neighbors in the neighbor table for all interfaces on this router.

**Related Commands**

Command	Description
<a href="#">show pim interface, on page 249</a>	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

XR EXEC

.

## Syntax Description

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
-------------	---

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 30: 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

XR EXEC

```
show pim [vrf vrf-name] [ipv4|ipv6] range-list [autorp| config] [ ip-address-name ]
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>config</b>	(Optional) Displays PIM command-line interface (CLI) range list information.
<i>ip-address-name</i>	(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

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 31: 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
<a href="#">show pim group-map, on page 247</a>	Displays group-to-PIM mode mapping.



# 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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance associated with this count.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

## Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

## Command Modes

EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 five 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 40 100000 100000
Topology Interface States 371 300000 300000
SM Registers 0 20000 20000
Group Ranges from AutoRP 3 100

```

This table describes the significant fields shown in the display.

**Table 32: 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.
Group Ranges from AutoRP	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.

# 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

XR EXEC

mode.

**show pim** [**vrf** *vrf-name*] [**ipv4|ipv6**] **topology** [*src-ip-address/grp-address*]

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

## Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 271.

**Note**

For forwarding information, use the **show mfib route** and **show mrrib 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 33: show pim topology Field Descriptions**

Field	Description
(11.0.0.1,239.9.9.9)SPT	Entry state. Source address, group address, and tree flag (shortest path tree or rendezvous point tree) for the route entry. Note that the tree flag may be missing from the entry.
SM	Entry protocol. PIM protocol mode in which the entry operates: sparse mode (SM), source specific multicast (SSM), bidirectional (BD), or dense-mode (DM).
Up: 00:00:13	Entry uptime. Time (in hours, minutes, and seconds) this entry has existed in the topology table.
RP: 11.0.0.1*	Entry information. Additional information about the route entry. If route entry is a sparse mode or bidirectional PIM route, the RP address is given.
JP: Null(never)	Entry join/prune state. Indicates if and when a join or prune message is sent to the RPF neighbor for the route.

Field	Description
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
<b>Entry Information Flags</b>	
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 list from an (*, G) route, the route entry LH flag appears only on the (*, G) route.
IA - Inherit Alive	Flag that indicates a source VPN routing and forwarding (VRF) route with the KAT active.
DSS - Don't Signal Sources	Flag that may be set on the last-hop (*, G) entries that indicates that new matching sources should not be signaled from the forwarding plane.
DCC - Don't Check Connected	Flag that is set when the KAT probes, which indicates that the connected check for new sources should be omitted in the forwarding plane.

Field	Description
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".
<b>Interface Information Flags</b>	
LI - Local Interest	Flag that indicates that there are local receivers for this entry on this interface, as reported by Internet Group Management Protocol (IGMP).
LD - Local Disinterest	Flag that indicates that there is explicit disinterest for this entry on this interface, as reported by IGMP exclude mode reports.
II - Internal Interest	Flag that indicates that the host stack of the router has internal receivers for this entry.
ID - Internal Disinterest	Flag that indicates that the host stack of the router has explicit internal disinterest for this entry.

Field	Description
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 XR EXEC mode.

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

## Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

## Command Modes

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 mrrib 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
```

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 33: show pim topology Field Descriptions, on page 267](#) 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
<b>show mfib route</b>	Displays all entries in the MFIB table.
<b>show mrif route</b>	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 XR EXEC mode.

```
show pim [vrf vrf-name] [ipv4| ipv6] topology entry-flag flag [detail| route-count]
```

## Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
flag	Configures a display of routes with the specified entry flag. Valid flags are the following: <ul style="list-style-type: none"> <li>• <b>AA</b> —Assume alive</li> <li>• <b>DCC</b> —Don't check connected</li> <li>• <b>DSS</b> —Don't signal sources</li> <li>• <b>E</b> —MSDP External</li> <li>• <b>EX</b> —Extranet flag set</li> <li>• <b>IA</b> —Inherit except flag set</li> <li>• <b>KAT</b> —Keepalive timer</li> <li>• <b>LH</b> —Last hop</li> <li>• <b>PA</b> —Probe alive</li> <li>• <b>RA</b> —Really alive</li> <li>• <b>RR</b> —Registered receiver</li> <li>• <b>SR</b> —Sending registers</li> </ul>
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

XR EXEC

**Command History**

Release	Modification
Release 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 mrrib 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 33: show pim topology Field Descriptions, on page 267](#) 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
<b>show mrrib route</b>	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.

XR EXEC

**show pim** [**vrf** *vrf-name*] [**ipv4**|**ipv6**] **topology interface-flag** *flag* [**detail**|**route-count**]

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>flag</i>	Configures a display of routes with the specified interface flag. Valid flags are the following:
<b>detail</b>	(Optional) Displays details about the interface flag information.
<b>route-count</b>	(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

XR EXEC

### Command History

Release	Modification
Release 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 mrrib route** commands.

## Task ID

Task ID	Operations
multicast	read

## Examples

The following is sample output from the **show pim topology interface-flag LI** 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 33: show pim topology Field Descriptions, on page 267](#) 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
<b>show mrrib route</b>	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 XR EXEC

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
ipv4	(Optional) Specifies IPv4 address prefixes.
detail	(Optional) Displays details about the summary information.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is ope

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 mrrib 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 271.

# show pim traffic

To display Protocol Independent Multicast (PIM) traffic counter information, use the **show pim traffic** command in mode  
XR EXEC

**show pim** [*vrf vrf-name*] [*ipv4| ipv6*] **traffic**

Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

XR EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Valid PIM Packets Received Sent
Hello              9207    15214426
                  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 34: 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 <b>clear pim counters</b> 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.

**Related Commands**

Command	Description
<a href="#">clear pim counters</a> , on page 202	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 XR EXEC

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional)	Specifies a VPN routing and forwarding (VRF) instance.
<b>ipv4</b>	(Optional)	Specifies IPv4 address prefixes.
<i>interface-unit</i>		Name of virtual tunnel interface that represents the encapsulation tunnel or the decapsulation tunnel.
<b>all</b>		Specifies both encapsulation and decapsulation tunnel interfaces.
<b>netio</b>	(Optional)	Displays information obtained from the Netio DLL.

<b>Command Default</b>	IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.
------------------------	---

<b>Command Modes</b>	XR EXEC
----------------------	---------

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

<b>Usage Guidelines</b>	<p>To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.</p>
-------------------------	--

PIM register packets are sent through the virtual encapsulation tunnel interface from the source's first-hop designated router (DR) router to the rendezvous point (RP). On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to sparse mode (SM), not to Source Specific Multicast (SSM)

Task ID	Task ID	Operations
	multicast	read

## Examples

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

```
RP/0/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 35: 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

<b>group-list</b> <i>access-list</i>	(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 5.0.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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	<b>allow-override</b>	(Optional) Allows SSM ranges to be overridden by more specific ranges.
	<b>disable</b>	(Optional) Disables SSM group ranges.
	<b>range access-list</b>	(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 address-family configuration  
Multicast VPN configuration

Command History	<b>Release</b>	<b>Modification</b>
	Release 5.0.0	This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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)# mcast-routing  
RP/0/RP0/CPU0:router(config-mcast)# ssm range 4
```





## Multicast Tool and Utility Commands on

---

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* in .

- [mrinfo](#), page 292
- [mtrace](#), page 294
- [sap cache-timeout](#), page 296
- [sap listen](#), page 297
- [show sap](#), page 299

# 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

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>host-address</b>	Can be either the Domain Name System (DNS) name or IP address of a multicast router entered in <i>A.B.C.D</i> format.  <b>Note</b> If omitted, the router queries itself.
<i>source-address</i>	(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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<b>vrf</b>	(Optional) Specifies the vrf table for the route lookup.
<i>source</i>	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.
<i>destination</i>	DNS name or address of the unicast destination. This is a unicast address of the end of the path to be traced.
<i>group_addr</i>	(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 <i>weak mtrace</i> . 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.
<i>resp_addr</i>	(Optional) DNS name or multicast address of the response address to receive response.
<i>ttl</i>	(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 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.



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	
<i>minutes</i>	Time that a SAP cache entry is active in the cache. Range is 1 to 1440.

Command Default	<i>minutes</i> : 1440 (24 hours)
-----------------	----------------------------------

Command Modes	Global configuration XR Config
---------------	-----------------------------------

Command History	Release	Modification
	Release 5.0.0	This command was introduced.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
------------------	---

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 XR 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

<i>ip-address</i>	(Optional) Group IP address for an address range.
<i>name</i>	(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

XR Config

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<a href="#">show sap, on page 299</a>	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

XR EXEC

**show sap [ipv4] [group-address| session-name] [detail]**

## Syntax Description

<b>ipv4</b>	(Optional) Specifies IPv4 address prefixes.
<i>group-address</i>	(Optional) Group IP address or name of the session that is learned.
<i>session-name</i>	(Optional) Session name.
<b>detail</b>	(Optional) Provides more SAP information.

## Command Default

IPv4 addressing is the default.

## Command Modes

EXEC

XR EXEC

## Command History

Release	Modification
Release 5.0.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 36: 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:mls
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 37: show sap detail Field Descriptions**

Field	Description
Session Name	Descriptive name of the SAP session.
Description	An expanded description of the session.

Field	Description
Group	IP multicast group addresses used for this session.
Announcement source	IP address of the host from which this session announcement was received.
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
<a href="#">sap listen</a> , on page 297	Configures the SDR listener on a group IP address.

show sap





## INDEX

### A

accept-register command [191](#)  
access-group (IGMP/MLD) command [3](#)  
accounting per-prefix command [113](#)  
accounting per-prefix forward-only command [115](#)  
address-family (multicast) command [117](#)  
auto-rp candidate-rp command [193](#)

### B

boundary command [120](#)  
bsr candidate-bsr command [198](#)  
bsr candidate-rp command [200](#)  
bsr-border command [196](#)

### C

cache-sa holdtime command [59](#)  
cache-sa-state command [61](#)  
clear igmp counters command [5](#)  
clear igmp group command [7](#)  
clear igmp reset command [9](#)  
clear mfib counter command [121](#)  
clear mfib database command [123](#)  
clear mfib hardware adjacency-counters command [124](#)  
clear msdp peer command [63](#)  
clear msdp sa-cache command [65](#)  
clear msdp stats command [67](#)  
clear pim counters command [202](#)  
clear pim topology command [205](#)  
connect-source command [69](#)

### D

default-peer command [71](#)  
description (peer) command [73](#)  
disable (multicast) command [125](#)

dr-priority command [207](#)

### E

enable (multicast) command [127](#)  
explicit-tracking command [11](#)

### F

forwarding-latency command [129](#)

### G

global maximum command [209](#)

### H

hello-interval (PIM) command [211](#)

### I

interface (multicast) command [131](#)  
interface (PIM) command [213](#)  
interface all enable command [133](#)  
interface-inheritance disable command [135](#)

### J

join-group command [13](#)  
join-prune-interval command [215](#)

**L**

log-traps command [137](#)

**M**

maximum disable command [138](#)  
 maximum external-sa command [75](#)  
 maximum groups command [15](#)  
 maximum groups-per-interface command [17](#)  
 maximum peer-external-sa command [77](#)  
 maximum register-states command [217](#)  
 maximum route-interfaces command [219](#)  
 maximum routes command [221](#)  
 mdt data command [139](#)  
 mdt default command [141](#)  
 mdt mtu command [143](#)  
 mdt source command [145](#)  
 mesh-group (peer) command [79](#)  
 mhost default-interface command [147](#)  
 mofrr command [223](#)  
 mrinfo command [292](#)  
 mtrace command [294](#)  
 multicast-routing command [149](#)

**N**

neighbor-check-on-recv enable command [225](#)  
 neighbor-check-on-send enable command [226](#)  
 neighbor-filter command [227](#)  
 nsf (multicast) command [151](#)  
 nsf lifetime (IGMP)nsf lifetime (IGMP/MLD) command [20](#)  
 nsf lifetime (PIM) command [228](#)

**O**

old-register-checksum command [230](#)  
 oom-handling command [153](#)  
 originator-id command [81](#)

**P**

password (peer) command [83](#)  
 peer (MSDP) command [85](#)

**Q**

query-interval command [22](#)

query-max-response-time command [24](#)  
 query-timeout command [26](#)

**R**

rate-per-route command [155](#)  
 remote-as (multicast) command [87](#)  
 robustness-count command [28](#)  
 router command [29](#)  
 router igmp command [31](#)  
 router pim command [232](#)  
 rp-address command [234](#)  
 rp-static-deny command [239](#)  
 rpf topology route-policy command [236](#)  
 rpf-vector command [238](#)

**S**

sa-filter command [88](#)  
 sap cache-timeout command [296](#)  
 sap listen command [297](#)  
 show auto-rp candidate-rp command [240](#)  
 show igmp groups command [33](#)  
 show igmp interface command [35](#)  
 show igmp nsf command [39](#)  
 show igmp ssm map command [44](#)  
 show igmp summary command [41](#)  
 show igmp traffic command [46](#)  
 show mfib connections command [156](#)  
 show mfib counter command [158](#)  
 show mfib encap-info command [160](#)  
 show mfib hardware route accept-bitmap command [162](#)  
 show mfib hardware route olist command [164](#)  
 show mhost default-interface command [166](#)  
 show mhost groups command [168](#)  
 show mrrib client command [170](#)  
 show mrrib nsf command [173](#)  
 show mrrib route command [175](#)  
 show mrrib route outgoing-interface command [179](#)  
 show mrrib route-collapse command [177](#)  
 show mrrib table-info command [181](#)  
 show mrrib tlc command [183](#)  
 show msdp globals command [90](#)  
 show msdp peer command [93](#)  
 show msdp rpf command [96](#)  
 show msdp sa-cache command [98](#)  
 show msdp statistics peer command [103](#)  
 show msdp summary command [105](#)  
 show pim context command [242](#)  
 show pim context table command [245](#)  
 show pim group-map command [247](#)

show pim interface command [249](#)  
show pim join-prune statistic command [252](#)  
show pim mstatic command [254](#)  
show pim neighbor command [256](#)  
show pim nsf command [259](#)  
show pim range-list command [261](#)  
show pim summary command [263](#)  
show pim topology command [265](#)  
show pim topology detail command [271](#)  
show pim topology entry-flag command [274](#)  
show pim topology interface-flag command [277](#)  
show pim topology summary command [280](#)  
show pim traffic command [282](#)  
show pim tunnel info command [285](#)  
show sap command [299](#)  
shutdown (MSDP) command [107](#)  
spt-threshold infinity command [287](#)

ssm command [288](#)  
ssm map static command [50](#)  
static-group command [52](#)

## T

ttl-threshold (MSDP) command [109](#)  
ttl-threshold (multicast) command [185](#)

## V

version command [54](#)  
vrf (igmp) command [56](#)  
vrf (multicast) command [187](#)

