CONTENTS

PREFACE

Preface ix
Changes to this Document ix
Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

IGMP Commands 1
access-group (IGMP) 2
clear igmp counters 4
clear igmp group 6
clear igmp reset 8
explicit-tracking 9
join-group 11
maximum groups 13
maximum groups-per-interface 16
nsf lifetime (IGMP) 19
query-interval 21
query-max-response-time 23
robustness-count 25
router 26
router igmp 28
show igmp groups 30
show igmp interface 32
show igmp nsf 36
show igmp summary 38
show igmp ssm map 41
show igmp traffic 42
ssm map 45
### CHAPTER 2

**Multicast Source Discovery Protocol Commands**

- static-group 46
- version 48
- cache-sa holdtime 52
- cache-sa-state 53
- clear msdp peer 55
- clear msdp sa-cache 56
- clear msdp stats 58
- connect-source 59
- default-peer 61
- description (peer) 62
- maximum external-sa 63
- maximum peer-external-sa 65
- mesh-group (peer) 67
- originator-id 68
- password (peer) 69
- peer (MSDP) 71
- remote-as (multicast) 72
- sa-filter 73
- show msdp globals 75
- show msdp peer 77
- show msdp rpf 79
- show msdp sa-cache 81
- show msdp statistics peer 85
- show msdp summary 87
- shutdown (MSDP) 89
- ttl-threshold (MSDP) 90

### CHAPTER 3

**Multicast Routing and Forwarding Commands**

- accounting per-prefix 94
- boundary 95
- clear mfib counter 96
- clear mfib database 97
CHAP TER 4

Multicast PIM Commands 139

accept-register 141
auto-rp candidate-rp 142
auto-rp mapping-agent 144
bsr candidate-bsr 146
clear pim counters 148
clear pim topology 151
dr-priority 153
global maximum bsr crp-cache threshold 155
hello-interval (PIM)  157
interface (PIM)  159
join-prune-interval  161
join-prune-mtu  163
maximum register-states  164
maximum route-interfaces  165
maximum routes  166
neighbor-check-on-recv enable  167
neighbor-check-on-send enable  168
neighbor-filter  169
nsf lifetime (PIM)  170
old-register-checksum  172
router pim  173
rp-address  175
rpf topology route-policy  177
rpf-redirect  178
rpf-redirect bundle  179
rpf-vector  181
rp-static-deny  182
show auto-rp candidate-rp  183
show pim global summary  185
show pim group-map  187
show pim interface  189
show pim join-prune statistic  192
show pim rpf-redirect  194
show pim rpf-redirect route  195
show pim mstatic  196
show pim nsf  198
show pim range-list  200
show pim traffic  202
show pim tunnel info  205
spt-threshold infinity  207
ssm  208
CHAPTER 5  Multicast Tool and Utility Commands  211

- mrinfo  212
- mtrace  214
- sap cache-timeout  216
- sap listen  217
- show sap  218
Preface

The Preface contains these topics:

• Changes to this Document, on page ix
• Obtaining Documentation and Submitting a Service Request, on page ix

Changes to this Document

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2013</td>
<td>Initial release of this document.</td>
</tr>
<tr>
<td>January 2014</td>
<td>Republished with documentation updates for Release 5.0.1 features.</td>
</tr>
<tr>
<td>August 2014</td>
<td>Republished with documentation updates for Release 5.2.1 features.</td>
</tr>
<tr>
<td>January 2015</td>
<td>Republished with documentation updates for Release 5.2.3 features.</td>
</tr>
<tr>
<td>November 2016</td>
<td>Republished with documentation updates for Release 6.1.2 features.</td>
</tr>
<tr>
<td>July 2017</td>
<td>Republished with documentation updates for Release 6.2.2 features.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished with documentation updates for Release 6.3.2 and Release 6.4.1 features.</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

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

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the RSS feeds are a free service.
IGMP Commands

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), on page 2
- clear igmp counters, on page 4
- clear igmp group, on page 6
- clear igmp reset, on page 8
- explicit-tracking, on page 9
- join-group, on page 11
- maximum groups, on page 13
- maximum groups-per-interface, on page 16
- nsf lifetime (IGMP), on page 19
- query-interval, on page 21
- query-max-response-time, on page 23
- robustness-count, on page 25
- router, on page 26
- router igmp, on page 28
- show igmp groups, on page 30
- show igmp interface, on page 32
- show igmp nsf, on page 36
- show igmp summary, on page 38
- show igmp ssm map, on page 41
- show igmp traffic, on page 42
- ssm map, on page 45
- static-group, on page 46
- version, on page 48
access-group (IGMP)

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

```
access-group access-list
no access-group access-list
```

**Syntax Description**

<table>
<thead>
<tr>
<th>access-list</th>
<th>Number or name of a standard IP access list. Range is 1 to 99.</th>
</tr>
</thead>
</table>

**Command Default**

No default behavior or values

**Command Modes**

IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 access-list</td>
<td>Defines a standard IP access list. For information, see <em>IP Addresses and Services Command Reference for Cisco NCS 6000 Series Routers</em></td>
</tr>
</tbody>
</table>
clear igmp counters

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

clear igmp [ipv4 | ] counters

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 addressing. IPv4 is the default for Internet Group Management Protocol (IGMP) groups.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Valid IGMP Packets</th>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Reports</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Leaves</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DVMRP packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PIM packets</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid IGMP Packets</td>
<td>0</td>
</tr>
<tr>
<td>Queries</td>
<td>0</td>
</tr>
<tr>
<td>Reports</td>
<td>0</td>
</tr>
<tr>
<td>Leaves</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace packets</td>
<td>0</td>
</tr>
<tr>
<td>DVMRP packets</td>
<td>0</td>
</tr>
<tr>
<td>PIM packets</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp traffic, on page 42</td>
<td>Displays all the Internet Group Management Protocol (IGMP) traffic-related counters.</td>
</tr>
</tbody>
</table>
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 | }] group [{ip-address | type interface-path-id}]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
- `ip-address` (Optional) IP hostname or group address.
- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` (Optional) Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

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

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp groups</code>, on page 30</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>


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 | ] reset`

**Syntax Description**

| **ipv4** | (Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups. |

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th><strong>Task ID</strong></th>
<th><strong>Operations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp groups</code>, on page 30</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through IGMP</td>
</tr>
<tr>
<td><code>show mrib route</code></td>
<td>Displays all route entries in the MRIB table.</td>
</tr>
</tbody>
</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` \(\{\text{access-list}\}\text{\|\text{disable}}\)  
`no` `explicit-tracking`

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list</code></td>
<td>(Optional) Access list that specifies the group range for host tracking.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>(Optional) Disables explicit host tracking on a specific interface. This option is available only in interface configuration mode.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

- IGMP interface configuration
- MLD configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show igmp groups, on page 30</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
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.

**Syntax**

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

**Syntax Description**

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

**Command Default**

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

**Command Modes**

IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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
```
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

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Maximum number of groups accepted by a router. Range is 1 to 20000.</td>
</tr>
</tbody>
</table>

### Command Modes

IGMP configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display the number of groups (39) and the maximum number of groups configured (20000). Through use of the `maximum groups` command, a configuration is committed to change the maximum number of groups to 40. Before and after configuration, the `show igmp summary` command is used to confirm the configuration change:

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

IGMP summary
```
Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 20000

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RSP0/CPU0/0</td>
<td>0</td>
<td>20000</td>
</tr>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-POS24</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/0</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/1</td>
<td>5</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/2</td>
<td>5</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/1/0/1</td>
<td>5</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/4/2</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/1</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/2</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/7</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/0/1</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/4/4</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/4/5</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/4/6</td>
<td>3</td>
<td>20000</td>
</tr>
</tbody>
</table>

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

% Failed to commit one or more configuration items during an atomic operation, no changes have been made. Please use 'show configuration failed' to view the errors

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

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

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

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

RP/0/RP0/CPU0:router# show igmp summary

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

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RP0/CPU0/0</td>
<td>0</td>
<td>20000</td>
</tr>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-POS24</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/0</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/1</td>
<td>5</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/2</td>
<td>5</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/1/0/1</td>
<td>5</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/1/4/2</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/1</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/2</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/7</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/0/1</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/4/4</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/4/5</td>
<td>3</td>
<td>20000</td>
</tr>
<tr>
<td>POS0/6/4/6</td>
<td>3</td>
<td>20000</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum groups-per-interface, on page 16</td>
<td>Configures the maximum number of groups for each interface accepted by a router.</td>
</tr>
<tr>
<td>show igmp summary, on page 38</td>
<td>Displays group membership information for Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
maximum groups-per-interface

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

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

Syntax Description

| number | Maximum number of groups accepted by a router for each interface. |

Command Default

number : 20000

Command Modes

IGMP configuration
IGMP interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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        |
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum groups, on page 13</td>
<td>Configures the maximum number of groups used by Internet Group Management Protocol (IGMP).</td>
</tr>
<tr>
<td>show igmp summary, on page 38</td>
<td>Displays group membership information for Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
**nsf lifetime (IGMP)**

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

```
nsf lifetime seconds
no nsf lifetime
```

**Syntax Description**

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

**Command Default**

- `seconds`: 60

**Command Modes**

- IGMP configuration

**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.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nfs (multicast)</code></td>
<td>Enables NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>nfs lifetime (PIM)</code></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><code>show igmp nfs, on page 36</code></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><code>show mfib nfs</code></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
</tbody>
</table>
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**
- `seconds` Frequency used to send IGMP host-query messages. Range is 1 to 3600.

**Command Default**
- If this command is not specified in interface configuration mode, the interface adopts the query interval parameter specified in IGMP configuration mode.
- If this command is not specified in IGMP configuration mode, the query interval time is 60 seconds.

**Command Modes**
- IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` 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.
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.

Note

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hello-interval (PIM)</code></td>
<td>Configures the frequency of PIM hello messages.</td>
</tr>
<tr>
<td><code>query-timeout</code></td>
<td>Configures the timeout value before the router takes over as the querier for the interface.</td>
</tr>
<tr>
<td><code>show igmp groups</code>, on page 30</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through IGMP.</td>
</tr>
</tbody>
</table>
query-max-response-time

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

```plaintext
query-max-response-time seconds
no query-max-response-time
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

- IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello-interval (PIM)</td>
<td>Configures the frequency of PIM hello messages.</td>
</tr>
<tr>
<td>show igmp groups, on page 30</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through IGMP.</td>
</tr>
</tbody>
</table>
robustness-count

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

```
robustness-count count
no robustness-count
```

**Syntax Description**
- `count`: Value of the robustness count variable. Range is 2 to 10 packets.

**Command Default**
Default is 2 packets.

**Command Modes**
IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**
- **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**

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

**Command Modes**

- IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 multicast-routing command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>multicast routing</strong></td>
<td>Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.</td>
</tr>
</tbody>
</table>
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 History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface all disable</td>
<td>Disables IGMP membership tracking on all interfaces.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>multicast routing</td>
<td>Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.</td>
</tr>
</tbody>
</table>
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 groups [ { group-address | type interface-path-id | not-active | summary } ] [ detail | explicit ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-address</td>
<td>(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.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>(Optional) Either a physical interface or a virtual interface.</td>
</tr>
<tr>
<td>not-active</td>
<td>(Optional) Displays group joins that are not processed.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the total number of (*, G) and (S, G) states in IGMP.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detail information such as IGMP Version 3 source list, host, and router mode.</td>
</tr>
<tr>
<td>explicit</td>
<td>(Optional) Displays explicit tracking information.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values

### Command Modes

- EXEC
- XR EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

### 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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp interface, on page 32</code></td>
<td>Displays Internet Group Management Protocol (IGMP) multicast-related information about an interface.</td>
</tr>
</tbody>
</table>
**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 interface [type interface-path-id|state-on|state-off]
```

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** (Optional) Either a physical interface or a virtual interface. **Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

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

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

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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/R0/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

Multicast Command Reference for the Cisco NCS 6000 Series Routers
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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>query-interval, on page 21</td>
<td>Configures the frequency at which Cisco IOS XR software sends IGMP host-query messages.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>router, on page 26</td>
<td>Enables or disables IGMP membership tracking.</td>
</tr>
</tbody>
</table>
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 nsf
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>old-output</td>
<td>(Optional) Displays the old show output—available for backward compatibility.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast read</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing state</td>
<td>Multicast NSF status of IGMP (Normal or Non-Stop Forwarding Activated).</td>
</tr>
<tr>
<td>NSF Lifetime</td>
<td>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).</td>
</tr>
<tr>
<td>NSF Time Remaining</td>
<td>If IGMP NSF state is activated, the time remaining until IGMP reverts to Normal mode displays.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf (multicast)</code></td>
<td>Enables NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>nsf lifetime (IGMP)</code>, on page 19</td>
<td>Configures the NSF timeout value for the IGMP or MLD process.</td>
</tr>
<tr>
<td><code>nsf lifetime (PIM)</code></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><code>show mfib nsf</code></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
<tr>
<td><code>show mrib nsf</code></td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td><code>show pim nsf</code></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
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 summary
```

**Syntax Description**
- `old-output` (Optional) Displays the old show output—available for backward compatibility.

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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

MgmtEth0/RP1/CPU0/0 0 5

3 5

5

5

5

3 5

/ / /

5

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

5

/ /

5

/6/ 3 5
/6/
This table describes the significant fields shown in the display.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Group x Interfaces</td>
<td>Number of multicast groups that are joined through the interface.</td>
</tr>
<tr>
<td>Maximum number of Group x Interfaces</td>
<td>Maximum number of multicast groups that can be joined through the interface.</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>Interfaces through which the multicast groups are reachable.</td>
</tr>
<tr>
<td>Unsupported Interfaces</td>
<td>Number of unsupported interfaces.</td>
</tr>
<tr>
<td>Enabled Interfaces</td>
<td>Number of enabled interfaces.</td>
</tr>
<tr>
<td>Disabled Interfaces</td>
<td>Number of disabled interfaces.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp groups, on page 30</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
show igmp ssm map

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

```
show igmp ssm map [group-address] [detail]
```

**Syntax Description**
- `group-address` (Optional) Specifies the address of the SSM group for which to obtain the mapping state.
- `detail` (Optional) Displays detailed source information.

**Command Default**
No default behavior or values

**Command Modes**
- EXEC
- 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.

**Task ID**
- **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 traffic
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid IGMP Packet</td>
<td>2784</td>
</tr>
<tr>
<td>Queries</td>
<td>0</td>
</tr>
<tr>
<td>Reports</td>
<td>2784</td>
</tr>
<tr>
<td>Leaves</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace packets</td>
<td>0</td>
</tr>
<tr>
<td>PIM packets</td>
<td>0</td>
</tr>
</tbody>
</table>

Errors:
```
This table describes the significant fields shown in the display for the `show igmp traffic` command.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Valid IGMP Packet            | Total number of valid protocol packets sent and received. Valid packet types include:  
  - Queries  
  - Membership reports  
  - Leaves                                                                                                                                                                                                                                                                                                                                 |
| Queries                      | Total number of query packets sent and received. IP Multicast routers send queries to determine the multicast reception state of neighboring interfaces.                                                                                                                                                                                                 |
| Reports                      | Total number of membership report packets received. Membership reports indicate either the current multicast reception state of a neighboring interface or a change to that state.                                                                                                                                                                                                                            |
| Leaves                       | Total number of leaves received. A leave group packet indicates a neighboring interface no longer has multicast reception state for a particular group.                                                                                                                                                                                                 |
| Mtrace packets               | Total number of Mtrace packets sent and received. Mtrace traces the route from a receiver to a source using a particular multicast address.                                                                                                                                                                                                 |
| PIM packets                  | Total number of sent and received Protocol Independent Multicast (PIM) packets.                                                                                                                                                                                                                                                                 |
| Malformed Packets            | Total number of malformed packets received. A malformed packet is a packet smaller than the smallest valid protocol packet.                                                                                                                                                                                                                                                                           |
| Bad Checksums               | Total number of packets received with a bad protocol header checksum.                                                                                                                                                                                                                                                                                                                                 |
| Socket Errors               | Total number of read and write failures on the protocol socket.                                                                                                                                                                                                                                                                                                                                 |
| Bad Scope Errors            | Total number of packets received with an invalid multicast scope. **Note**: IGMP has no invalid scopes; this counter, therefore, never increments in IGMP.                                                                                                                                                                                                 |
| Auxiliary Data Len Errors    | Total number of packets received with a non-zero auxiliary data length.                                                                                                                                                                                                                                                                                                                                 |
| Subnet Errors               | Total number of packets received that were not sourced on the same subnet as the router.  
  MTRACE packets received are not checked for this error as they may be validly sourced from a different subnet.                                                                                                                                                                                                                           |
Total number of packets dropped due to an invalid socket.

Total number of packets that could not be sent or received. This might occur if:
- Packet buffer does not form a valid protocol packet.
- IP header is not written to the packet.
- Outgoing packet interface handle was not set.
- Errors occurred calculating the protocol checksum.

Packets dropped for any other reason.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim traffic</td>
<td>Displays PIM traffic counter information.</td>
</tr>
</tbody>
</table>
ssm map

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

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

**Syntax Description**

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

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

**Syntax Description**

- `group-address` (IP address of the multicast group in IPv4 prefixing format):
  - IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format `A.B.C.D`.

- `inc-mask mask` (Optional) Specifies a mask for the increment range. This is an IP address expressed range in IPv4 format. This mask is used with the group address to generate subsequent group addresses:
  - IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format `A.B.C.D`.

  **Note** This mask is used with the group address to generate subsequent group addresses.

- `count cnt` (Optional) Specifies a number of group addresses to generate using the increment mask. Range is 1 to 512.

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

**Command Default**

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

**Command Modes**

IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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:

```sh
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.
- 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 configuration mode.

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

**Command Modes**

- IGMP configuration
- IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>query-max-response-time, on page 23</td>
<td>Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.</td>
</tr>
</tbody>
</table>
version
Multicast Source Discovery Protocol Commands

This chapter describes the commands used to configure and monitor the Multicast Source Discovery Protocol (MSDP) on Cisco NCS 6000 Routers.

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, on page 52
• cache-sa-state, on page 53
• clear msdp peer, on page 55
• clear msdp sa-cache, on page 56
• clear msdp stats, on page 58
• connect-source, on page 59
• default-peer , on page 61
• description (peer), on page 62
• maximum external-sa, on page 63
• maximum peer-external-sa, on page 65
• mesh-group (peer), on page 67
• originator-id, on page 68
• password (peer), on page 69
• peer (MSDP), on page 71
• remote-as (multicast), on page 72
• sa-filter, on page 73
• show msdp globals, on page 75
• show msdp peer, on page 77
• show msdp rpf , on page 79
• show msdp sa-cache, on page 81
• show msdp statistics peer, on page 85
• show msdp summary, on page 87
• shutdown (MSDP), on page 89
• ttl-threshold (MSDP), on page 90
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.

**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 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cache-sa-state, on page 53</code></td>
<td>Controls cache source-active (SA) state on a router.</td>
</tr>
</tbody>
</table>
**cache-sa-state**

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

```
cache-sa-state {list access-list-number|rp-list access-list-name}

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

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

**Command Default**
The router creates SA state.

**Command Modes**
MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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-mdp)# cache-sa-state list 100
RP/0/RP0/CPU0:router(config-mdp)# 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
```
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.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show msdp sa-cache, on page 81</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>ipv4</th>
<th>(Optional) Specifies IPv4 address prefixes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-address</td>
<td>IPv4 address or hostname of the MSDP peer to which the TCP connection is cleared.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router# clear msdp peer 224.15.9.8
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 71</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
clear msdp sa-cache

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced,</td>
</tr>
</tbody>
</table>

**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**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>
```

**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:
clear msdp sa-cache

RP/0/RP0/CPU0:router# clear msdp sa-cache 224.5.6.7

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp sa-cache, on page 81</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
<td></td>
</tr>
</tbody>
</table>
clear msdp stats

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

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

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

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- **Release** 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.

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

```
RP/0/RP0/CPU0:router# clear msdp stats peer 224.0.1.1
```

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show msdp statistics peer</code>, on page 85</td>
<td>Displays Multicast Source Discovery Protocol (MSDP) peer statistic counters.</td>
</tr>
</tbody>
</table>
connect-source

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

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

**Syntax Description**
- `type` (Interface type. For more information, use the question mark (?) online help function.)
- `interface-path-id` (Optional) Physical interface or virtual interface.

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

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

**Command Modes**
- MSDP configuration
- MSDP peer configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**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: multicast
  - Read: read,
  - Write: write
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address or Domain Name System (DNS) name of the MSDP default peer.</td>
</tr>
</tbody>
</table>

**Command Default**

No default MSDP peer exists.

**Command Modes**

MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 71</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
description (peer)

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

```
description peer-address text
no description peer-address text
```

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

**Command Default**
No description is associated with an MSDP peer.

**Command Modes**
MSDP peer configuration

**Command History**
- Release 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
```

**Related Commands**
- **Command**: peer (MSDP), on page 71
  - Description: Configures a Multicast Source Discovery Protocol (MSDP) peer.
- **Command**: show msdp peer, on page 77
  - Description: Displays information about the Multicast Source Discovery Protocol (MSDP) peer.
**maximum external-sa**

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

```
maximum external-sa entries
no maximum external-sa
```

**Syntax Description**

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

**Command Default**

- **entries**: 20000

**Command Modes**

- MSDP peer configuration
- MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 MSPD peer to override the maximum external SA entry value configured with the `maximum peer-external-sa` command.

**Note**

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum peer-external-sa, on page 65</td>
<td>Configures the maximum number of external Multicast Source Discovery Protocol (MSDP) Source-Active (SA) entries that can be learned from MSDP peers.</td>
</tr>
<tr>
<td>show msdp summary, on page 87</td>
<td>Displays Multicast Source Discovery Protocol (MSDP) peer status.</td>
</tr>
</tbody>
</table>
maximum peer-external-sa

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

```
maximum peer-external-sa entries
no maximum peer-external-sa
```

**Syntax Description**

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

**Command Default**

- `entries : 20000`

**Command Modes**

- MSDP configuration

**Command History**

```
Release Modification
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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>maximum external-sa, on page 63</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>show msdp summary, on page 87</td>
<td>Displays Multicast Source Discovery Protocol (MSDP) peer status.</td>
</tr>
</tbody>
</table>
mesh-group (peer)

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

```
mesh-group name
no mesh-group name
```

**Syntax Description**
- `name`: Name of the mesh group.

**Command Default**
MSDP peers do not belong to a mesh group.

**Command Modes**
MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.0.0</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```
originator-id type interface-path-id
no originator-id type interface-path-id
```

**Syntax Description**

- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or virtual interface.

**Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
The RP address is used as the originator ID.

**Command Modes**
MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure Gigabit Ethernet interface 0/1/0 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 GigE0/1/0
```
password (peer)

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

```
password {clear|encrypted} password
no password {clear|encrypted} password
```

**Syntax Description**

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

**Command Default**

No password is configured.

**Command Modes**

MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show msdp peer, on page 77</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
peer (MSDP)

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

```
peer peer-address
no peer peer-address
```

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

**Command Default**
No MSDP peer is configured.

**Command Modes**
MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**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# configure
RP/0/RP0/CPU0(config)# router msdp
RP/0/RP0/CPU0(config-router)# peer 172.16.1.2
RP/0/RP0/CPU0(config-router-internal)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-peer</code>, on page 61</td>
<td>Defines a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) source-active (SA) messages.</td>
</tr>
</tbody>
</table>
remote-as (multicast)

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

```
remote-as as-number
no remote-as as-number
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

```
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`in</td>
<td>out`</td>
</tr>
<tr>
<td><code>list access-list-name</code></td>
<td>Specifies an IP access list number or name. If no access list is specified, no (S, G) pairs from the peer are filtered.</td>
</tr>
<tr>
<td><code>rp-list access-list-name</code></td>
<td>Specifies an originating rendezvous point (RP) access list in SA messages.</td>
</tr>
</tbody>
</table>

### Command Default

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

### Command Modes

- MSDP configuration
- MSDP peer configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 71</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
</tbody>
</table>

### Command Default

IPv4 addressing is the default.

### Command Modes

XR EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

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

```
RP/0/RPI0/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 (Total, Active)
                      | ADV/RPF      |
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 alloced/free: 1/0
Total RP buffers alloced/free: 2/0
TLV buffers alloced/free: 1/1

This table describes the significant fields shown in the display.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>Local autonomous system.</td>
</tr>
<tr>
<td>caching</td>
<td>SA caching that is enabled.</td>
</tr>
<tr>
<td>originator</td>
<td>Local rendezvous point (RP).</td>
</tr>
<tr>
<td>default peer</td>
<td>Default peer to accept Source Active (SA) messages from when all Reverse Path Forwarding (RPF) rules fail.</td>
</tr>
<tr>
<td>Active RP</td>
<td>All RPs involved in sending SA messages to this router.</td>
</tr>
<tr>
<td>Grange/len</td>
<td>Multicast Group Range or Multicast Group Mask.</td>
</tr>
<tr>
<td>Source Count</td>
<td>Total and active SA messages advertised by the respective RP.</td>
</tr>
<tr>
<td>ADV/RPF</td>
<td>Advertiser and RPF entry.</td>
</tr>
<tr>
<td>Max/active group count</td>
<td>Maximum group count since router was booted and number of active groups.</td>
</tr>
<tr>
<td>Max/active SA count</td>
<td>Maximum SA message count since router was booted, and number of active SA messages.</td>
</tr>
<tr>
<td>Total source buffers alloced/free</td>
<td>Number of internal source buffers allocated and freed after allocation.</td>
</tr>
<tr>
<td>Total group buffers alloced/free</td>
<td>Number of internal group buffers allocated and freed after allocation.</td>
</tr>
<tr>
<td>Total RP buffers alloced/free</td>
<td>Number of internal RP buffers allocated and freed after allocation.</td>
</tr>
<tr>
<td>TLV buffers alloced/free</td>
<td>Number of internal time-to-live buffers allocated and freed after allocation.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp, on page 77</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp sa-cache, on page 81</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
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**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `peer-address` (Optional) IP address or hostname of the MSDP peer for which information is displayed.

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

**Command Modes**
- XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` `read`
- `Task ID` `multicast`

**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

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 71</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp sa-cache, on page 81</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP peer for 172.16.1.1 is 10.1.1.1</td>
<td>IP address of the MSDP RPF peer.</td>
</tr>
<tr>
<td>AS 200</td>
<td>Autonomous system to which the peer belongs.</td>
</tr>
<tr>
<td>rule: 1</td>
<td>MSDP RPF rule that matches what was learned from SAs.</td>
</tr>
<tr>
<td>bgp/rib lookup:</td>
<td>Multicast RPF routing table lookup.</td>
</tr>
<tr>
<td>nexthop: 10.1.1.1</td>
<td>Router where the SA is sent to reach the final destination.</td>
</tr>
<tr>
<td>asnum: 200</td>
<td>Autonomous system number for the next-hop neighbor router.</td>
</tr>
</tbody>
</table>
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**

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

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

### Examples

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

```plaintext
RP/0/RP0/CPU0# 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 recv 1049, Encapsulated data received: 0
grp flags: Pt, src flags: E, EA, PI
```

This table describes the significant fields shown in the display.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10.10.5.102, 239.1.1.1)</td>
<td>The first address (source) is sending to the second address (group).</td>
</tr>
<tr>
<td>RP 10.10.4.3</td>
<td>Rendezvous point (RP) address in the originating domain where the SA messages started.</td>
</tr>
<tr>
<td>MBGP/AS 20</td>
<td>RP is in autonomous system AS 20 according to the unicast RPF table:</td>
</tr>
<tr>
<td></td>
<td>• If Multiprotocol Border Gateway Protocol (MBGP) is not configured—RIB table 1.</td>
</tr>
<tr>
<td></td>
<td>• If MBGP is configured—RIB table 2 or multicast table.</td>
</tr>
<tr>
<td>15:44:03/00:01:17</td>
<td>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.</td>
</tr>
<tr>
<td>Encapsulated data received: 0</td>
<td>MSDP SA captures any data information when the source starts so that the receiver does not miss data when the SA path is established.</td>
</tr>
</tbody>
</table>

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

```plaintext
RP/0/RP0/CPU0# 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 recv 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(*, 239.1.1.1)</td>
<td>Protocol Independent Multicast (PIM) interest in the group due to a local Internet Group Management Protocol (IGMP) join.</td>
</tr>
<tr>
<td>RP 0.0.0.0</td>
<td>There is no RP associated with this entry.</td>
</tr>
<tr>
<td>AS 0</td>
<td>This entry is 0, autonomous system (AS) rendezvous point (RP) is null.</td>
</tr>
<tr>
<td>06:32:18/expired</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Originator-RP</th>
<th>SA total</th>
<th>RPF peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.1</td>
<td>0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>172.17.1.1</td>
<td>3</td>
<td>172.17.1.1</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # of SAs</td>
<td>Total number of SAs that are currently active in the system.</td>
</tr>
<tr>
<td>Total # of RPs</td>
<td>Total number of RPs that have distributed the SA information to this system.</td>
</tr>
<tr>
<td>Total # of Sources</td>
<td>Total number of sources that are active from all domains.</td>
</tr>
<tr>
<td>Total # of Groups</td>
<td>Total number of groups to which sources are sending data from all domains.</td>
</tr>
<tr>
<td>Originator-RP</td>
<td>SA information based on the individual RPs and the originating domains that distributed them.</td>
</tr>
</tbody>
</table>

Multicast Command Reference for the Cisco NCS 6000 Series Routers

83
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
(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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cache-sa-state</code>, on page 53</td>
<td>Controls cache source-active (SA) state on a router.</td>
</tr>
<tr>
<td><code>peer (MSDP)</code>, on page 71</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>peer-address</td>
<td>(Optional) IP address or name of the MSDP peer.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear msdp stats, on page 58</td>
<td>Resets Multicast Source Discovery Protocol (MSDP) peer statistic counters.</td>
</tr>
</tbody>
</table>
show msdp summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the `show msdp summary` command in

XR EXEC

Syntax Description

```
show msdp [ipv4] summary
```

**ipv4** (Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

XR EXEC

Command History

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

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  Peer  Active  Cfg.Max  TLV
Peer Cnt Ext.SAs  recv/sent
---                 --  ----  ------- ----------  ----  ----  -------  -------  ----
10.1.1.1            0 NoIntf  00:10:07  0       ?  0  0       0       0/0
```
This table describes the significant fields shown in the display.

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp peer, on page 77</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp sa-cache, on page 81</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp peer, on page 77</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
**ttl-threshold (MSDP)**

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

```
ttl-threshold ttl
no ttl-threshold ttl
```

**Syntax Description**
```
ttl Time to live value. Range is 1 to 255.
```

**Command Default**
```
ttl : 1
```

**Command Modes**
- MSDP configuration
- MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

- `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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 71</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
ttl-threshold (MSDP)
Multicast Routing and Forwarding Commands

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

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

- accounting per-prefix, on page 94
- boundary, on page 95
- clear mfib counter, on page 96
- clear mfib database, on page 97
- disable (multicast), on page 98
- enable (multicast), on page 100
- forwarding-latency, on page 102
- interface (multicast), on page 103
- interface all enable, on page 105
- interface-inheritance disable, on page 107
- log-traps, on page 109
- maximum disable, on page 110
- multicast-routing, on page 111
- nsf (multicast), on page 112
- oom-handling, on page 114
- rate-per-route, on page 115
- show mfib connections, on page 116
- show mfib counter, on page 118
- show mrrib cofo, on page 120
- show mfib hardware route accept-bitmap, on page 122
- show mfib hardware route olist, on page 123
- show mrrib cofo, on page 125
- show mrrib client, on page 127
- show mrrib nsf, on page 130
- show mrrib route, on page 132
- show mrrib route-collapse, on page 134
- show mrrib table-info, on page 136
- ttl-threshold (multicast), on page 137
accounting per-prefix

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

`accounting per-prefix`
`no accounting per-prefix`

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

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

**Command Modes**
Multicast routing configuration
Multicast routing address family IPv4 and IPv6 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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.

**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
```
boundary

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

```
boundary access-list
no boundary access-list
```

### Syntax Description

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

### Command Default

A multicast boundary is not configured.

### Command Modes

Multicast routing interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 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 [{ipv4|ipv6}] counter [{group-addresssource-address}] [location {node-id|all}]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `group-address` (Optional) IP address of the multicast group.
- `source-address` (Optional) IP address of the source of the multicast route.
- `location node-id` (Optional) Clears route packet counters from the designated node.
- `all` The `all` keyword clears route packet counters on all nodes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

To clear the Multicast Forwarding Information Base (MFIB) database, use the `clear mfib database` command in the appropriate mode.

```
clear mfib [{ipv4|ipv6}] database [{location {node-id|all}}]
```

**Syntax Description**

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

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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
```
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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
```
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable (multicast), on page 98</td>
<td>Disables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>interface all enable, on page 105</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
forwarding-latency

To delay traffic being forwarded on a route, use the `forwarding-latency` command. To return to the default behavior, use the `no` form of this command.

```
forwarding-latency [delay milliseconds]
no forwarding-latency
```

**Syntax Description**

- `delay milliseconds` (Optional) Specifies the delay time in milliseconds. Range is 5 - 500.

**Command Default**

The default delay time is 30 milliseconds.

**Command Modes**

- Multicast routing configuration
- IPv4 multicast routing configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

- `multicast` read, write

**Examples**

The following example shows how to delay traffic from being forwarded for 120 milliseconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router# forwarding-latency delay 120
```
interface (multicast)

To configure multicast interface properties, use the `interface` command in the appropriate configuration mode. To disable multicast routing for interfaces, use the `no` form of this command.

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

- `type`: Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id`: Physical interface or virtual interface.

**Notes**

- Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.
- For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

- Multicast routing configuration
- IPv4 or multicast routing configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable (multicast), on page 98</td>
<td>Disables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>enable (multicast), on page 100</td>
<td>Enables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>interface all enable, on page 105</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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:

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable (multicast), on page 98</td>
<td>Disables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>enable (multicast), on page 100</td>
<td>Enables multicast routing and forwarding on an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```
Note
```

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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.

```
Multicast Command Reference for the Cisco NCS 6000 Series Routers
```
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 default address-family ipv4
interface Loopback0
  enable

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

```
router igmp
  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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

**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

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

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
```
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords or arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>No default behavior or values.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>XR Config</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 5.0.0 This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting per-prefix, on page 94</td>
<td>Enables per-prefix counters only in hardware.</td>
</tr>
<tr>
<td>alias</td>
<td>Creates a command alias.</td>
</tr>
<tr>
<td>interface (multicast), on page 103</td>
<td>Configures multicast interface properties.</td>
</tr>
<tr>
<td>interface all enable, on page 105</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
nsf (multicast)

To turn on the nonstop forwarding (NSF) capability for the multicast routing system, use the `nsf` command in multicast routing configuration mode. To turn off this function, use the `no` form of this command.

```
nsf [lifetime seconds]
no nsf [lifetime]
```

**Syntax Description**

- `lifetime seconds` (Optional) Specifies the maximum time (in seconds) for NSF mode. Range is 30 to 3600.

**Command Default**

This command is disabled by default.

**Command Modes**

- Multicast routing configuration
- Multicast routing address family ipv4 configuration

**Command History**

- **Release** 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 (MFWD) partner processes by MRIB. MRIB remains in NSF mode until Internet Group Management Protocol (IGMP) has recovered state from the network and host stack and until PIM has recovered state from the network and IGMP. When both PIM and IGMP have recovered and fully updated the MRIB, MRIB signals the MFIBs that NSF is ending, and begins updating the stale MFIB entries. When all updates have been sent, the MFWD partner processes delete all remaining stale MFIB entries and returns to normal operation, ending the NSF mode. MFIB NSF timeout prior to the signal from MRIB may cause NSF to end, and thus forwarding to stop.

When forwarding is in NSF mode, multicast flows may continue longer than necessary when network conditions change due to multicast routing protocols, unicast routing protocol reachability information, or local sender
and receiver changes. The MFWD partner processes halt forwarding on stale MFIB entries when the potential for a multicast loop is detected by receipt of incoming data on a forwarding interface for the matching MFIB entry.

**Note**
For NSF to operate successfully in your multicast network, you must also enable NSF for the unicast protocols (such as Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF] and Border Gateway Protocol [BGP]) that PIM relies on for Reverse Path Forwarding (RPF) information. See the appropriate configuration modules to learn how to configure NSF for unicast protocols.

### Task ID
**Task ID** | **Operations**
--- | ---
multicast | read, write

### Examples
The following example shows how to enable NSF for the multicast routing system:

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

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>nsf lifetime (IGMP)</strong></td>
<td>Configures the maximum time for the NSF timeout value under IGMP.</td>
</tr>
<tr>
<td><strong>nsf lifetime (PIM)</strong></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><strong>show igmp nsf</strong></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><strong>show mfib nsf</strong></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
<tr>
<td><strong>show mrib nsf, on page 130</strong></td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td><strong>show pim nsf</strong></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim topology</td>
<td>Displays PIM topology table information.</td>
</tr>
</tbody>
</table>
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable individual route calculations:

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

```
show mfib [[ipv4|ipv6]] connections [location node-id]
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `location node-id` (Optional) Specifies MFIB connections associated with an interface of the designated node.

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

**Command Modes**
- XR EXEC
- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysDB-NSF</td>
<td>connected</td>
</tr>
<tr>
<td>SYSDB-EDM</td>
<td>connected</td>
</tr>
<tr>
<td>SYSDB-Action</td>
<td>connected</td>
</tr>
<tr>
<td>A1B</td>
<td>connected</td>
</tr>
<tr>
<td>MLIB</td>
<td>connected</td>
</tr>
<tr>
<td>IDB</td>
<td>connected</td>
</tr>
<tr>
<td>IIR</td>
<td>connected</td>
</tr>
<tr>
<td>IPARM</td>
<td>connected</td>
</tr>
<tr>
<td>GSP</td>
<td>connected</td>
</tr>
</tbody>
</table>
show mfib counter

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

```
show mfib [ipv4|ipv6] counter [location node-id]
```

**Syntax Description**

**ipv4**
(Optional) Specifies IPv4 address prefixes.

**ipv6**
(Optional) Specifies IPv6 address prefixes.

**location node-id**
(Optional) Specifies MFIB counter statistics associated with an interface of the designated node.

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

**Command Modes**
EXEC
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets [no input idb]</td>
<td>Packets dropped because no input interface information was found in the packet.</td>
</tr>
<tr>
<td>Packets [failed route lookup]</td>
<td>Packets dropped because of failure to match any multicast route.</td>
</tr>
<tr>
<td>Packets [Failed idb lookup]</td>
<td>Packets dropped because the descriptor block was not found for an interface (incoming or outgoing).</td>
</tr>
<tr>
<td>Packets [Mcast disabled on input I/F]</td>
<td>Packets dropped because arriving on an interface that was not enabled for the multicast routing feature.</td>
</tr>
<tr>
<td>Packets [encap drops due to ratelimit]</td>
<td>Packets dropped because of rate limit.</td>
</tr>
</tbody>
</table>
show mrib cofo

To display collapsed forwarding route information for the Multicast Rorwarding Information Base (MRIB) process, use the `show mrib cofo` command in XR EXEC mode.

```
show mrib {encap-id number | lsm label number | ip-multicast ip-address/prefix | summary }
```

**Syntax Description**

- `encap-id number` (Optional) Specifies encapsulation-id number.
- `lsm label number` (Optional) Specifies LSM information.
- `ip-multicast ip-address/prefix` (Optional) Specifies IP multicast information.
- `summary` (Optional) Specifies COFO multicast database summary.

**Command Default**

None.

**Command Modes**

XR EXEC

**Command History**

Release 6.4.1  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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output is from the `show mfib cofo summary` command:

```
RP/0/RP0/CPU0:router# show mrib cofo summary

MRIB COFO DB Summary:
Type | Local | Remote
--- | --- | ---
Number of (*,G) entries | 0 | 100
Number of (S,G) entries | 0 | 0
Number of label entries | 0 | 0
Number of encap entries | 0 | 0
```

In the above output, Remote entries show collapsed route from remote SDR.

The following sample output is from the `show mfib cofo ip-multicast` command:

```
RP/0/RP0/CPU0:router# sh mrib cofo ip-multicast 226.1.1.1/32
MRIB Collapsed Forwarding DB -- IP Multicast Info: (*,226.1.1.1)
```
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 [[ipv4|ipv6]] hardware route accept-bitmap [*] [source-address] [group-address [/prefix-length]] [detail] [location node-id]
```

### Syntax Description
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- ***** (Optional) Displays shared tree entry.
- **source-address** (Optional) IP address or hostname of the multicast route source:
- **group-address** (Optional) IP address or hostname of the multicast group.
- **/ prefix-length** (Optional) Prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
- **location node-id** Specifies an MFIB-designated node.

### Command Default
IPv4 addressing is the default.

### Command Modes
XR EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
# 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 [{ipv4|ipv6}] hardware route olist {[*] | [source-address] [group-address [/prefix-length]] [detail]} [location node-id]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
<tr>
<td>*</td>
<td>(Optional) Displays shared tree entries.</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional) IP address or hostname of the multicast route source.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) IP address or hostname of the multicast group.</td>
</tr>
<tr>
<td>/ prefix-length</td>
<td>(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.</td>
</tr>
<tr>
<td>location node-id</td>
<td>Specifies an MFIB-designated node.</td>
</tr>
</tbody>
</table>

## Command Default

IPv4 addressing is the default.

## Command Modes

XR EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
The following is sample output from the `show mfb hardware route olist` command for line card 0/1/CPU0 (the output fields are described in the header):

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

<table>
<thead>
<tr>
<th>Source Group</th>
<th>M</th>
<th>C</th>
<th>RPF</th>
<th>FU</th>
<th>FGID</th>
<th>P</th>
<th>PF</th>
<th>BA</th>
<th>Interface</th>
<th>IC</th>
<th>OP</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 224.0.0.0</td>
<td>4</td>
<td>T</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>41785 F</td>
<td>F</td>
<td>T</td>
<td>True</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 224.0.0.0</td>
<td>24</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>47206 F</td>
<td>F</td>
<td>T</td>
<td>True</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 224.0.1.39</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>47205 T</td>
<td>F</td>
<td>F</td>
<td>True</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 224.0.1.40</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>27202 T</td>
<td>F</td>
<td>F</td>
<td>True</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 232.0.0.0</td>
<td>8</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>47207 F</td>
<td>F</td>
<td>T</td>
<td>True</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 233.1.0.0</td>
<td>16</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>44106 F</td>
<td>F</td>
<td>T</td>
<td>False NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 233.1.0.0</td>
<td>16</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>44106 F</td>
<td>F</td>
<td>T</td>
<td>False NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 233.1.0.0</td>
<td>16</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>44106 F</td>
<td>F</td>
<td>T</td>
<td>False PO0/1/0 F</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>* 233.1.1.1</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>27205 F</td>
<td>F</td>
<td>T</td>
<td>False NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 233.1.1.1</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>27205 F</td>
<td>F</td>
<td>T</td>
<td>False PO0/1/1 F</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>* 233.1.1.1</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>27205 F</td>
<td>F</td>
<td>T</td>
<td>False PO0/1/0 F</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>* 233.1.1.2</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>27206 F</td>
<td>F</td>
<td>T</td>
<td>False Po0/1/1 F</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>* 233.1.1.2</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>27206 F</td>
<td>F</td>
<td>T</td>
<td>False Po0/1/0 F</td>
<td>F</td>
<td></td>
</tr>
</tbody>
</table>
```
show mrib cofo

To display collapsed forwarding route information for the Multicast Rorwarding Information Base (MRIB) process, use the **show mrib cofo** command in XR EXEC mode.

```
show mrib { encap-id number | lsm label number | ip-multicast ip-address/prefix | summary }
```

**Syntax Description**

- **encap-id number** (Optional) Specifies encapsulation-id number.
- **lsm label number** (Optional) Specifies LSM information.
- **ip-multicast ip-address/prefix** (Optional) Specifies IP multicast information.
- **summary** (Optional) Specifies COFO multicast database summary.

**Command Default**

None.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 sample output is from the **show mrib cofo summary** command:

```
RP/0/RP0/CPU0:router# show mrib cofo summary

MRIB COFO DB Summary:
Type | Local | Remote
---|---|---
Number of (*,G) entries | 0 | 100|
Number of (S,G) entries | 0 | 0|
Number of label entries | 0 | 0|
Number of encap entries | 0 | 0|
```

In the above output, **Remote** entries show collapsed route from remote SDR.

The following sample output is from the **show mrib cofo ip-multicast** command:

```
RP/0/RP0/CPU0:router# show mrib cofo ip-multicast 226.1.1.1/32
MRIB Collapsed Forwarding DB -- IP Multicast Info: (*,226.1.1.1)
```
show mrib cofo

Origin: REMOTE
Receive Count: 1
Last Received: Thu Oct 12 03:18:55 2017
Node set: 0/3/1
(2.8.1.2,226.1.1.1)

Origin: REMOTE
Receive Count: 1
Last Received: Thu Oct 12 04:13:30 2017
Node set: 0/3/1
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 [ipv4|ipv6] [old-output] client [filter] [client-name]
```

**Syntax Description**
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **filter** (Optional) Displays route and interface level flag changes that various MRIB clients have registered and shows what flags are owned by the MRIB clients.
- **client-name** (Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as Protocol Independent Multicast (PIM) or Internet Group Management Protocol (IGMP).

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

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**
- **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

This table describes the significant fields shown in the display.

**Table 16: show mrib client Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp</td>
<td>Name of the client.</td>
</tr>
<tr>
<td>417957</td>
<td>Personal identifier (PID) or a unique ID assigned by MRIB.</td>
</tr>
<tr>
<td>(connection id 0)</td>
<td>Unique client connection identifier.</td>
</tr>
<tr>
<td>ownership filter:</td>
<td>Specifies all the route entry and interface-level flags that are owned by</td>
</tr>
<tr>
<td></td>
<td>the client. As the owner of the flag, only the client can add or remove the</td>
</tr>
<tr>
<td></td>
<td>flag. For example, only the Internet Group Management Protocol (IGMP) client</td>
</tr>
<tr>
<td></td>
<td>can add the II flag on an interface. MRIB does not allow a non-owner to</td>
</tr>
<tr>
<td></td>
<td>register or modify the same flag.</td>
</tr>
<tr>
<td>groups: include</td>
<td>Groups and interfaces registered by the clients consisting of two lists.</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>One is an include list (items for which the client requests to be notified.)</td>
</tr>
<tr>
<td>interfaces: include All</td>
<td>The use of “All” implies all interfaces and 0.0.0.0/0 to indicate all</td>
</tr>
<tr>
<td></td>
<td>groups. Not shown in this example is the exclude list. This list contains</td>
</tr>
<tr>
<td></td>
<td>items for which the client requests not to be notified when modifications</td>
</tr>
<tr>
<td></td>
<td>occur.</td>
</tr>
<tr>
<td>interface attributes:</td>
<td>Interface-level flags set on the interface belong to a route.</td>
</tr>
<tr>
<td>II ID LI LD</td>
<td></td>
</tr>
<tr>
<td>interest filter:</td>
<td>Specifies all the flags, groups, and interfaces from which the client</td>
</tr>
<tr>
<td></td>
<td>requests information. When a flag of interest for a client is modified, the</td>
</tr>
<tr>
<td></td>
<td>client is notified.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>entry attributes:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S C I A IF D</td>
<td>Entry-level flags that are set on the route.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show mrib nsf</strong>, on page 130</td>
<td>Displays the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
show mrib nsf

To display the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB), use the `show mrib nsf` command in the appropriate mode.

```
show mrib [{ipv4|ipv6}] [old-output] nsf
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

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

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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 17: show mrib nsf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing state</td>
<td>Multicast NSF status of the MRIB (Normal or NSF Activated).</td>
</tr>
<tr>
<td>NSF Lifetime</td>
<td>Timeout for MRIB NSF, computed as the maximum of the PIM and Internet Group Management Protocol (IGMP) NSF lifetimes, plus 60 seconds.</td>
</tr>
<tr>
<td>NSF Time Remaining</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsf (multicast), on page 112</td>
<td>Configures the NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td></td>
<td>Configures the maximum time for the NSF timeout value under IGMP.</td>
</tr>
<tr>
<td>nsf lifetime (PIM)</td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td>show igmp nsf</td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td>show mfib nsf</td>
<td>Displays the state of NSF operation in the MFIB line cards.</td>
</tr>
<tr>
<td>show pim nsf</td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
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 [ {ipv4|ipv6} ] [old-output] route [ {summary|outgoing-interface} [ { * source-address } ] [ group-address [ / prefix-length ]] ] [ detail ]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `*` (Optional) Displays shared tree entries.
- `source-address` (Optional) Source IP address or hostname of the MRIB route. Format is: `A.B.C.D` or `X:X::X`.
- `group-address` (Optional) Group IP address or hostname of the MRIB route. Format is: `A.B.C.D` or `X:X::X`.
- `/prefix-length` (Optional) Prefix length of the MRIB group address. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Format is: `A.B.C.D` or `X:X::X`.
- `outgoing-interface` (Optional) Displays the outgoing-interface information.
- `summary` (Optional) Displays a summary of the routing database.
- `detail` (Optional) Displays the routing database with the platform data.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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 118` command displays global counters independent of the routes.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib counter, on page 118</td>
<td>Displays MFIB counter statistics for packets that have dropped.</td>
<td></td>
</tr>
<tr>
<td>show mrib route-collapse, on page 134</td>
<td>Displays the contents of the MRIB route collapse database.</td>
<td></td>
</tr>
</tbody>
</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 [ipv4|ipv6] route-collapse
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

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

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>nodeid</th>
<th>slot</th>
<th>refcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x20</td>
<td>0/2/CPU0</td>
<td>1</td>
</tr>
</tbody>
</table>

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
<table>
<thead>
<tr>
<th>nodeid</th>
<th>slot</th>
<th>refcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x20</td>
<td>0/2/CPU0</td>
<td>1</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show mrib route</strong>, on page 132</td>
<td>Displays all entries in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
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 [{{ipv4}|ipv6}] table-info
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

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

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router#
show mrib table-info
default [tid 0xe0000000]
Registered Client:
  igmp [ccb: 0 cltid: 4485366]
  pim [ccb: 1 cltid: 4485368]
  bcdl_agent [ccb: 2 cltid: 1]
  msdp [ccb: 3 cltid: 8827135]
```

**Table 18: show mrib table-info Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cltid</td>
<td>Client ID.</td>
</tr>
<tr>
<td>bcdl_agent</td>
<td>A process like igmp and pim, which is used to download routes to line card.</td>
</tr>
</tbody>
</table>
ttl-threshold (multicast)

To configure the time-to-live (TTL) threshold for packets being forwarded out an interface, use the `ttl-threshold` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
ttl-threshold  ttl
no  ttl-threshold  ttl
```

**Syntax Description**
- `ttl` Time to live value. Range is 1 to 255.

**Command Default**
- `ttl`: 0

**Command Modes**
- Multicast routing interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ttl-threshold (MSDP)</code></td>
<td>Limits which multicast data packets are sent in SA messages to an MSDP peer.</td>
</tr>
</tbody>
</table>
Multicast PIM Commands

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, on page 141
- auto-rp candidate-rp, on page 142
- auto-rp mapping-agent, on page 144
- bsr candidate-bsr, on page 146
- clear pim counters, on page 148
- clear pim topology, on page 151
- dr-priority, on page 153
- global maximum bsr crp-cache threshold, on page 155
- hello-interval (PIM), on page 157
- interface (PIM), on page 159
- join-prune-interval, on page 161
- join-prune-mtu, on page 163
- maximum register-states, on page 164
- maximum route-interfaces, on page 165
- maximum routes, on page 166
- neighbor-check-on-receive enable, on page 167
- neighbor-check-on-send enable, on page 168
- neighbor-filter, on page 169
- nsf lifetime (PIM), on page 170
- old-register-checksum, on page 172
- router pim, on page 173
- rp-address, on page 175
- rpf topology route-policy, on page 177
- rpf-redirect, on page 178
- rpf-redirect bundle, on page 179
- rpf-vector, on page 181
- rp-static-deny, on page 182
- show auto-rp candidate-rp, on page 183
- show pim global summary, on page 185
- show pim group-map, on page 187
• show pim interface, on page 189
• show pim join-prune statistic, on page 192
• show pim rpf-redirect, on page 194
• show pim rpf-redirect route, on page 195
• show pim mstatic, on page 196
• show pim nsf, on page 198
• show pim range-list, on page 200
• show pim traffic, on page 202
• show pim tunnel info, on page 205
• spt-threshold infinity, on page 207
• ssm, on page 208
accept-register

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

```
accept-register access-list-name
no accept-register
```

**Syntax Description**

```
access-list-name  Access list number or name.
```

**Command Default**

No default behavior or values

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>scope</td>
<td>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.</td>
</tr>
<tr>
<td>group-list access-list-name</td>
<td>(Optional) Specifies an access list that describes the group ranges for which this router is the rendezvous point.</td>
</tr>
<tr>
<td>interval seconds</td>
<td>(Optional) Specifies the time between rendezvous point announcements. Range is 1 to 600.</td>
</tr>
</tbody>
</table>

**Command Default**

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

*seconds*: 60

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### 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
```
auto-rp mapping-agent

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

**auto-rp mapping-agent** type interface-path-id scope ttl-value [interval seconds]
no auto-rp mapping-agent

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the show interfaces command in EXEC mode to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td>scope ttl-value</td>
<td>Specifies time-to-live (TTL) value in router hops that limits the scope of the rendezvous point discovery messages that are sent from that interface. Range is 1 to 255.</td>
</tr>
<tr>
<td>interval seconds</td>
<td>(Optional) Specifies the time, in seconds, between discovery messages. Range is 1 to 600.</td>
</tr>
</tbody>
</table>

**Command Default**

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

seconds : 60

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

More than one rendezvous point mapping agent can be configured in a network sending redundant information, for a slight increase in reliability.
The TTL value is used to limit the range, or scope, of a multicast transmission. Therefore, use this value only on border routers.

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

**Note**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-rp candidate-rp</code>, on page 142</td>
<td>Configures a router as a Protocol Independent Multicast (PIM) rendezvous point (RP) candidate that sends messages to the well-known CISCO-RP-ANNOUNCE multicast group (224.0.1.39).</td>
</tr>
</tbody>
</table>
bsr candidate-bsr

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

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

**Syntax Description**

- **ip-address**: IP address of the BSR router for the domain. For IPv4, this is an IP address in four-part dotted-decimal notation.

- **hash-mask-len length**: (Optional) Specifies the length of a mask that is to be used in the hash function.
  - All groups with the same seed hash (correspond) to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups.
  - For IPv4 addresses, we recommend a value of 30. The range is 0 to 32.

- **priority value**: (Optional) Specifies the priority of the candidate BSR. Range is 1 to 255. We recommend the BSR with the higher priority. If the priority values are the same, the router with the higher IP address is the BSR.

**Command Default**

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

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3</td>
<td>PIM BSR limits were introduced for this command.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
clear pim counters

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

```
clear pim counters
```

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router# show pim traffic
PIM Traffic Counters
Elapsed time since counters cleared: 1d01h

Received | Sent
---|---
Valid PIM Packets 15759217 | 15214426
Hello 9207 | 12336
Join-Prune 1076805 | 531981
Data Register 14673205 | 0
Null Register 73205 | 0
Register Stop 0 | 14673205
Assert 0 | 0
Batched Assert 0 | 0
Bidir DF Election 0 | 0
```
The table describes the significant fields shown in the display.

**Table 19: show pim traffic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time since counters cleared</td>
<td>Time (in days and hours) that had elapsed since the counters were cleared with the <em>clear pim counters</em> command.</td>
</tr>
<tr>
<td>Valid PIM Packets</td>
<td>Total PIM packets that were received and sent.</td>
</tr>
<tr>
<td>HelloJoin-PruneRegisterRegister StopAssert Bidir DF Election</td>
<td>Specific type of PIM packets that were received and sent.</td>
</tr>
<tr>
<td>Malformed Packets</td>
<td>Invalid packets due to format errors that were received and sent.</td>
</tr>
<tr>
<td>Bad Checksums</td>
<td>Packets received or sent due to invalid checksums.</td>
</tr>
<tr>
<td>Socket Errors</td>
<td>Packets received or sent due to errors from the router’s IP host stack sockets.</td>
</tr>
<tr>
<td>Packets dropped due to invalid socket</td>
<td>Packets received or sent due to invalid sockets in the router’s IP host stack.</td>
</tr>
<tr>
<td>Packets which couldn't be accessed</td>
<td>Packets received or sent due to errors when accessing packet memory.</td>
</tr>
<tr>
<td>Packets sent on Loopback Errors</td>
<td>Packets received or sent due to use of loopback interfaces.</td>
</tr>
<tr>
<td>Packets received on PIM-disabled Interface</td>
<td>Packets received or sent due to use of interfaces not enabled for PIM.</td>
</tr>
<tr>
<td>Packets received with Unknown PIM Version</td>
<td>Packets received or sent due to invalid PIM version numbers in the packet header.</td>
</tr>
</tbody>
</table>
PIM Traffic Counters
Elapsed time since counters cleared: 00:00:04

<table>
<thead>
<tr>
<th>Counter Type</th>
<th>Sent</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSR Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Candidate-RP Adv.</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join groups sent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Prune groups sent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Output JP bytes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Output hello bytes</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear pim counters</td>
<td>show pim traffic, on page 202</td>
<td>Displays Protocol Independent Multicast (PIM) traffic counter information.</td>
</tr>
</tbody>
</table>
clear pim topology

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

```
clear pim [ipv4|ipv6] topology [ip-address-name|reset]
```

**Syntax Description**
- **ipv4**: (Optional) Specifies IPv4 address prefixes.
- **ipv6**: (Optional) Specifies IPv6 address prefixes.
- **ip-address-name**: (Optional) Can be either one of the following:
  - Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host command.
  - IP address of the multicast group, in IPv4 format according to the specified address family.
- **reset**: (Optional) Deletes all entries from the topology table and resets the MRIB connection.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

XR EXEC

**Command History**

- **Release 5.0.0**
  - This command was introduced.
- **Release 5.2.1**
  - IPv6 support was added on this command.

**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.
### clear pim topology

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

```
RP/0/RP0/CPU0:router# clear pim topology
```
**dr-priority**

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

```
dr-priority value
no dr-priority
```

**Syntax Description**

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

**Command Default**

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

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

**Command Modes**

PIM interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 bsr crp-cache threshold

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

```
[global] maximum [{bsr crp-cache threshold}]
no [global] maximum [{bsr crp-cache threshold}]
```

### Syntax Description

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

### Command Default

No default behavior or values.

### Command Modes

PIM configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 bsr** command is used to the threshold limits for the crp-cache levels.

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

### Task ID

- **Task ID**
  - Operations
  - multicast read, write

### Examples

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

```
RP/0/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim)# address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# global maximum bsr crp-cache 2000 threshold 500
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum bsr crp-cache 1800 threshold 450
```

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

```
RP/0/RP0/CPU0:router# router pim
RP/0/RP0/CPU0:router(config-pim)# address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# global maximum bsr crp-cache 600 threshold 550
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# maximum bsr crp-cache 500 threshold 450
```
hello-interval (PIM)

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

```
hello-interval seconds
no hello-interval
```

**Syntax Description**

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

**Command Default**

Default is 30 seconds.

**Command Modes**

PIM interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr-priority, on page 153</td>
<td>Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.</td>
</tr>
</tbody>
</table>
interface (PIM)

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

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

- **type**: Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id**: Physical interface or virtual interface.

**Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr-priority, on page 153</td>
<td>Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.</td>
</tr>
<tr>
<td>hello-interval (PIM), on page 157</td>
<td>Configures the frequency of Protocol Independent Multicast (PIM) hello messages.</td>
</tr>
<tr>
<td>join-prune-interval, on page 161</td>
<td>Configures the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic.</td>
</tr>
</tbody>
</table>
**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.

```console
join-prune-interval seconds
no join-prune-interval
```

**Syntax Description**

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

**Command Default**

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

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

**Command Modes**

PIM interface configuration

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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:

```console
RP/0/RP0/CPU0:router(config)# router pim
```
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# join-prune-interval 90
join-prune-mtu

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

```
join-prune-mtu value
no join-prune-mtu value
```

**Syntax Description**

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

**Command Default**

65535 bytes

**Command Modes**

Router PIM configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

```
Task ID   Operation
---------|------------------
multicast| read, write
```

**Example**

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

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

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

maximum register-states number
no maximum register-states

**Syntax Description**

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

**Command Default**

number : 20000

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```
**maximum route-interfaces**

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

```
maximum route-interfaces number
no maximum route-interfaces
```

**Syntax Description**

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

**Command Default**

`number`: 30000

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```
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 maximum routes` command.

`maximum routes number`
`no maximum routes`

**Syntax Description**

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

**Command Default**

- `number`: 100000

**Command Modes**

- PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```
neighbor-check-on-recv enable

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

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

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

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

**Command Modes**
PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 on received join and prune messages:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor-check-on-send enable</code></td>
<td>Enables Protocol Independent Multicast (PIM) neighbor checking when sending join and prune messages.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor-check-on-recv enable</code>, on page 167</td>
<td>Blocks the receipt of join and prune messages from non-Protocol Independent Multicast (PIM) neighbors.</td>
</tr>
</tbody>
</table>
neighbor-filter

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

```
neighbor-filter access-list
no neighbor-filter
```

**Syntax Description**

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

**Command Default**

PIM neighbor messages are not filtered.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.0.0</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# neighbor-filter 1
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RP0/CPU0:router(config)# ipv4 access-list 1
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny ipv4 any 10.0.0.1/24
```
**nsf lifetime (PIM)**

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

```
nsf lifetime seconds
no nsf lifetime
```

**Syntax Description**

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

**Command Default**

- `seconds` : 120

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf (multicast)</code></td>
<td>Turns on NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>show igmp nsf</code></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><code>show mfib nsf</code></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
<tr>
<td><code>show mrib nsf</code></td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show pim nsf, on page 198</td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
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.

```plaintext
old-register-checksum
no old-register-checksum
```

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

**Command Default**
No default behavior or values

**Command Modes**
PIM configuration

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**
- **Task ID**:
  - multicast
- **Operations**:
  - 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:

```plaintext
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 access-list</td>
<td>Defines a standard IP access list. For more information, see IP Addresses and Services Command Reference for Cisco NCS 6000 Series Routers</td>
</tr>
</tbody>
</table>
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 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`.

**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
```
rpf-redirect

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

```
rpf-redirect route-policy policy-name
no rpf-redirect route-policy policy-name
```

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

**Command Default**
No default behavior or values

**Command Modes**
- PIM configuration
- PIM address-family configuration

**Command History**
- **Release 5.2.1**
  - This command was introduced.

**Usage Guidelines**
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*.

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

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim)#address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rpf-redirect route-policy <route-policy>
```
**rpf-redirect bundle**

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

- PIM configuration
- PIM address-family configuration
- Interface mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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*.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

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

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

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim)# address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# hello-interval 1
```
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# join-prune-interval 15
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rpf-redirect route-policy directv
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 60
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface GigabitEthernet0/0/4/7
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# enable
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# rpf-redirect bundle WEST bandwidth 6000 threshold 5000
rpf-vector

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

```
rpf-vector
no rpf-vector
```

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

**Command Default**
By default, RPF vector signaling is disabled.

**Command Modes**
PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

```
rp-static-deny access-list
no rp-static-deny
```

### Syntax Description

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

### Command Default

No default behavior or values

### Command Modes

PIM configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

- `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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 access-list</td>
<td>Defines a standard IP access list.</td>
</tr>
</tbody>
</table>
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

**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 20: show auto-rp candidate-rp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Range</td>
<td>Multicast group address and prefix for which this router is advertised as a rendezvous point.</td>
</tr>
<tr>
<td>Mode</td>
<td>PIM protocol mode for which this router is advertised as a rendezvous point, either PIM-SM or bidirectional PIM (bidir).</td>
</tr>
<tr>
<td>Candidate RP</td>
<td>Address of the interface serving as a rendezvous point for the range.</td>
</tr>
<tr>
<td>ttl</td>
<td>TTL scope value (in router hops) for Auto-RP candidate announcement messages sent out from this candidate rendezvous point interface.</td>
</tr>
<tr>
<td>interval</td>
<td>Time between candidate rendezvous point announcement messages for this candidate rendezvous point interface.</td>
</tr>
</tbody>
</table>
show pim global summary

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

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

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

```
RP/0/RP0/CPU0:router# show pim global summary

PIM Global Summary

PIM State Counters

<table>
<thead>
<tr>
<th>Field</th>
<th>Current</th>
<th>Maximum</th>
<th>Warning-threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>8</td>
<td>100000</td>
<td>100000</td>
</tr>
<tr>
<td>Topology Interface States</td>
<td>8</td>
<td>300000</td>
<td>300000</td>
</tr>
<tr>
<td>SM Registers</td>
<td>0</td>
<td>20000</td>
<td>20000</td>
</tr>
<tr>
<td>AutoRP Group Ranges</td>
<td>0</td>
<td>500</td>
<td>450</td>
</tr>
<tr>
<td>BSR Group Ranges</td>
<td>0</td>
<td>500</td>
<td>450</td>
</tr>
<tr>
<td>BSR C-RP caches</td>
<td>0</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

### Table 21: show pim global summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Topology Interface States</td>
<td>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.</td>
</tr>
<tr>
<td>SM Registers</td>
<td>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.</td>
</tr>
<tr>
<td>AutoRP Group Ranges</td>
<td>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.</td>
</tr>
<tr>
<td>Warning-threshold</td>
<td>Maximum number of multicast routes that can be configured per router.</td>
</tr>
<tr>
<td>BSR Group Ranges</td>
<td>The number of BSR groups and the maximum set range.</td>
</tr>
<tr>
<td>BSR C-RP caches</td>
<td>The number of candidate-RP caches in BSR and the maximum set range.</td>
</tr>
</tbody>
</table>
show pim group-map

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

```
show pim [{ipv4|ipv6}] group-map [ip-address-name] [info-source]
```

**Syntax Description**

- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **info-source** (Optional) Displays the group range information source.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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.

**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)

<table>
<thead>
<tr>
<th>Group Range</th>
<th>Proto</th>
<th>Client Groups</th>
<th>RP address</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.1.39/32*</td>
<td>DM</td>
<td>perm</td>
<td>1</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>224.0.1.40/32*</td>
<td>DM</td>
<td>perm</td>
<td>1</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
```
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 22: show pim group-map Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Range</td>
<td>Multicast group range that is mapped.</td>
</tr>
<tr>
<td>Proto</td>
<td>Multicast forwarding mode.</td>
</tr>
<tr>
<td>Client</td>
<td>States how the client was learned.</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups from the PIM topology table.</td>
</tr>
<tr>
<td>RP address</td>
<td>Rendezvous point address.</td>
</tr>
<tr>
<td>Info</td>
<td>RPF interface used and the PIM-SM Reverse Path Forwarding (RPF) information toward the rendezvous point.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain ipv4 host</td>
<td>Defines a static hostname-to-address mapping in the host cache using IPv4. For more information, see <em>IP Addresses and Services Command Reference for Cisco NCS 6000 Series Routers</em></td>
</tr>
<tr>
<td>rp-address, on page 175</td>
<td>Configures the address of a PIM rendezvous point for a particular group.</td>
</tr>
<tr>
<td>show pim range-list, on page 200</td>
<td>Displays the range-list information for PIM.</td>
</tr>
</tbody>
</table>
**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 ([ipv4|ipv6]) interface ([type interface-path-id|state-on|state-off]) [detail]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` (Optional) Displays only interfaces from which PIM is enabled and active.
- `state-on` (Optional) Displays only interfaces from which PIM is disabled or inactive.
- `state-off` (Optional) Displays detailed address information.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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  Operations
multicast  read

Examples

The following is sample output from the `show pim interface` command:

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

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>PIM</th>
<th>Nbr Count</th>
<th>Hello Intvl</th>
<th>DR</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.52.127</td>
<td>MgmtEth0/0/CPU0/0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.6.6.6</td>
<td>Loopback0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Loopback60</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.46.4.6</td>
<td>ATM0/2/0/0.1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.46.5.6</td>
<td>ATM0/2/0/0.2</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.46.6.6</td>
<td>ATM0/2/0/0.3</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.46.7.6</td>
<td>ATM0/2/0/0.4</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.46.8.6</td>
<td>ATM0/2/0/3.1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.46.9.6</td>
<td>ATM0/2/0/3.2</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.16.6</td>
<td>Serial0/3/2/1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.2</td>
<td>Serial0/3/0/0/0:0:0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.6</td>
<td>Serial0/3/0/0/1:0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.10</td>
<td>Serial0/3/0/2:0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.14</td>
<td>Serial0/3/0/2:1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.18</td>
<td>Serial0/3/0/3:0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.22</td>
<td>Serial0/3/0/3:1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.26</td>
<td>Serial0/3/0/3:2</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.4.30</td>
<td>Serial0/3/0/3:3</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.8.2</td>
<td>Serial0/3/0/1:0:0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.12.6</td>
<td>Serial0/3/2/0.1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.13.6</td>
<td>Serial0/3/2/0.2</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.14.6</td>
<td>Serial0/3/2/0.3</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.56.15.6</td>
<td>Serial0/3/2/0.4</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.67.4.6</td>
<td>POS0/4/1/0</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
<tr>
<td>10.67.8.6</td>
<td>POS0/4/1/1</td>
<td>off</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>not elected</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface type and number that is configured to run PIM.</td>
</tr>
<tr>
<td>PIM</td>
<td>PIM is turned off or turned on this interface.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Number of PIM neighbors in the neighbor table for the interface.</td>
</tr>
<tr>
<td>Hello Intvl</td>
<td>Frequency, in seconds, of PIM hello messages, as set by the <code>ip pim hello-interval</code> command in interface configuration mode.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>Designated router priority is advertised by the neighbor in its hello messages.</td>
</tr>
</tbody>
</table>
### Multicast Command Reference for the Cisco NCS 6000 Series Routers

#### show pim interface

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR</td>
<td>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.</td>
</tr>
</tbody>
</table>
show pim join-prune statistic

To display Protocol Independent Multicast (PIM) join and prune aggregation statistics, use the show pim join-prune statistic command in EXEC mode.

```
show pim [ipv4|ipv6] join-prune statistic [type interface-path-id]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>(Optional) Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the show interfaces command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

IP addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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 statistic 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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Interface</th>
<th>MTU</th>
<th>Transmitted</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback0</td>
<td>1514</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>Encapstunnel0</td>
<td>0</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>Decapstunnel0</td>
<td>0</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>Loopback1</td>
<td>1514</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>POS0/3/0/0</td>
<td>4470</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>POS0/3/0/3</td>
<td>4470</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

Table 24: `show pim join-prune statistics` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface from which statistics were collected.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) in bytes for the interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Number of join and prune states aggregated into transmitted messages in the last 1000/10000/50000 transmitted join and prune messages.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of join and prune states aggregated into received messages in the last 1000/10000/50000 received join and prune messages.</td>
</tr>
</tbody>
</table>
show pim rpf-redirect

To display the maximum bandwidth, the bandwidth used by traffic flowing through the local box, and the bandwidth used by other routers sharing the PIM bundle member interfaces of all members of bundles known to the system, use `show pim rpf-redirect` command in EXEC mode.

**Syntax Description**

```
show pim  ipv4  rpf-redirect
```

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

The following sample output from the `show pim rpf-redirect` command displays statistics about the PIM bundles:

```
RP/0/RP0/CPU0:router#show pim rpf-redirect

Mon Aug 11 16:50:35.811 IST

PIM RPF-Redirect bundle database

Member    Available/Allocated Bandwidth Threshold Bandwidth Local / Network Bandwidth Total Bandwidth
          (Kbps)             (Kbps)             (Kbps)

Bundle: east
Gi0/0/0/0  100000/100000  80000/80000  0/0       0
```

where, Available/Allocated Bandwidth (kbps) is the total multicast bandwidth (in kbps) available/allocated for multicast transmission; Available/Threshold Bandwidth (kbps) is the multicast bandwidth threshold beyond which the redirects are enabled, displays the available and the threshold bandwidth (kbps); Local/Network Bandwidth (in kbps) is the difference between the Allocated Bandwidth and Available Bandwidth; and the Total Bandwidth (kbps) is represented by the Local/Network Bandwidth.
show pim rpf-redirect route

To display the content of the snooping database, use show pim rpf-redirect command in EXEC mode.

show pim ipv4 rpf-redirect route

**Syntax Description**

| **IPv4** | (Optional) Specifies IPv4 address prefixes. |

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
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.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

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

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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 25: show pim mstatic Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td>pos0/1/0/1</td>
<td>Interface that is entered to reach destination IP address 10.0.0.1</td>
</tr>
<tr>
<td>172.16.0.1</td>
<td>Next-hop IP address to enter to reach destination address 10.0.0.1.</td>
</tr>
<tr>
<td>0</td>
<td>Distance of this mstatic route.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static-rpf</td>
<td>Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.</td>
</tr>
</tbody>
</table>
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


```
show pim [{ipv4|ipv6}] nsf
```

**Syntax Description**

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

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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 26: show pim nsf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing state</td>
<td>PIM state is in NSF recovery mode (Normal or Non-Stop Forwarding Activated).</td>
</tr>
<tr>
<td>NSF Lifetime</td>
<td>Total NSF lifetime (seconds, hours, and minutes) configured for PIM.</td>
</tr>
<tr>
<td>NSF Time Remaining</td>
<td>Time remaining in NSF recovery for PIM if NSF recovery is activated.</td>
</tr>
</tbody>
</table>
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 [{ipv4|ipv6}] range-list [{autorp|config}] [ip-address-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
<tr>
<td>config</td>
<td>(Optional) Displays PIM command-line interface (CLI) range list information.</td>
</tr>
<tr>
<td>ip-address-name</td>
<td>(Optional) IP address of the rendezvous point.</td>
</tr>
</tbody>
</table>

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

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**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
```
This table describes the significant fields shown in the display.

**Table 27: show pim range-list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Group range was learned by means of configuration.</td>
</tr>
<tr>
<td>SSM</td>
<td>PIM mode is operating in Source Specific Multicast (SSM) mode. Other modes are Sparse-Mode (SM) and bidirectional (BD) mode.</td>
</tr>
<tr>
<td>Exp: never</td>
<td>Expiration time for the range is “never”.</td>
</tr>
<tr>
<td>Src: 0.0.0.0</td>
<td>Advertising source of the range.</td>
</tr>
<tr>
<td>230.0.0.0/8</td>
<td>Group range: address and prefix.</td>
</tr>
<tr>
<td>Up: 03:47:09</td>
<td>Total time that the range has existed in the PIM group range table. In other words, the uptime in hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim group-map, on page 187</td>
<td>Displays group-to-PIM mode mapping.</td>
</tr>
</tbody>
</table>
**show pim traffic**

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

```
show pim  [{ipv4|ipv6}]  traffic
```

**Syntax Description**

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

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast  read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim traffic` command that displays a row for valid PIM packets, number of hello packets, and so on:

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

PIM Traffic Counters
Elapsed time since counters cleared: 1d01h

Received  Sent
Valid PIM Packets 15759217   15214426
Hello            9207         12336
Join-Prune       1076805      531981
Data Register    14673205     0
Null Register    73205        0
Register Stop    0            14673205
```
This table describes the significant fields shown in the display.

**Table 28: show pim traffic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time since counters cleared</td>
<td>Time (in days and hours) that had elapsed since the counters were cleared with the <code>clear pim counters</code> command.</td>
</tr>
<tr>
<td>Valid PIM Packets</td>
<td>Total PIM packets that were received and sent.</td>
</tr>
<tr>
<td>Hello</td>
<td>Specific type of PIM packets that were received and sent.</td>
</tr>
<tr>
<td>Bidir DF Election</td>
<td></td>
</tr>
<tr>
<td>Join</td>
<td></td>
</tr>
<tr>
<td>Prune</td>
<td></td>
</tr>
<tr>
<td>Register</td>
<td></td>
</tr>
<tr>
<td>Stop</td>
<td></td>
</tr>
<tr>
<td>Assert</td>
<td></td>
</tr>
<tr>
<td>Batched Assert</td>
<td></td>
</tr>
<tr>
<td>BSR Message</td>
<td></td>
</tr>
<tr>
<td>Candidate-RP Adv.</td>
<td></td>
</tr>
<tr>
<td>Join groups sent</td>
<td></td>
</tr>
<tr>
<td>Prune groups sent</td>
<td></td>
</tr>
<tr>
<td>Output JP bytes</td>
<td></td>
</tr>
<tr>
<td>Output hello bytes</td>
<td>4104</td>
</tr>
<tr>
<td>Malformed Packets</td>
<td>Invalid packets due to format errors that were received and sent.</td>
</tr>
<tr>
<td>Bad Checksums</td>
<td>Packets received or sent due to invalid checksums.</td>
</tr>
<tr>
<td>Socket Errors</td>
<td>Packets received or sent due to errors from the router’s IP host stack sockets.</td>
</tr>
<tr>
<td>Packets dropped due to invalid socket</td>
<td>Packets received or sent due to invalid sockets in the router’s IP host stack.</td>
</tr>
<tr>
<td>Packets which couldn't be accessed</td>
<td>Packets received or sent due to errors when accessing packet memory.</td>
</tr>
<tr>
<td>Packets sent on Loopback Errors</td>
<td>Packets received or sent due to use of loopback interfaces.</td>
</tr>
<tr>
<td>Packets received on PIM-disabled Interface</td>
<td>Packets received or sent due to use of interfaces not enabled for PIM.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Packets received with Unknown PIM Version</td>
<td>Packets received or sent due to invalid PIM version numbers in the packet header.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear pim counters, on page 148</code></td>
<td>Clears Protocol Independent Multicast (PIM) counters and statistics.</td>
</tr>
</tbody>
</table>
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 mode.

```
show pim [ipv4|ipv6] tunnel info {interface-unit|all} [netio]
```

**Syntax Description**

- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **interface-unit** Name of virtual tunnel interface that represents the encapsulation tunnel or the decapsulation tunnel.
- **all** Specifies both encapsulation and decapsulation tunnel interfaces.
- **netio** (Optional) Displays information obtained from the Netio DLL.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td>IPv6 support was added on this command.</td>
</tr>
</tbody>
</table>

**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 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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
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 29: show pim tunnel info Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the tunnel interface.</td>
</tr>
<tr>
<td>RP Address</td>
<td>IP address of the RP tunnel endpoint.</td>
</tr>
<tr>
<td>Source Address</td>
<td>IP address of the first-hop DR tunnel endpoint, applicable only to encapsulation interfaces.</td>
</tr>
</tbody>
</table>
spt-threshold infinity

To change the behavior of the last-hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the `spt-threshold infinity` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
spt-threshold infinity [group-list access-list]
no spt-threshold infinity
```

**Syntax Description**

- `group-list access-list` (Optional) Indicates the groups restricted by the access list.

**Command Default**

The last-hop Protocol Independent Multicast (PIM) router switches to the shortest-path source tree by default.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the PIM source group `grp1` to always use the shared tree:

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# spt-threshold infinity group-list grp1
```
ssm

To define the Protocol Independent Multicast (PIM)-Source Specific Multicast (SSM) range of IP multicast addresses, use the ssm command in the appropriate configuration mode. To return to the default behavior, use the no form of this command.

ssm [{allow-override|disable|range access-list}]
no ssm [{allow-override|disable|range}]

Syntax Description

- allow-override (Optional) Allows SSM ranges to be overridden by more specific ranges.
- disable (Optional) Disables SSM group ranges.
- range access-list (Optional) Specifies an access list describing group ranges for this router when operating in PIM SSM mode.

Command Default

Interface operates in PIM sparse mode (PIM-SM). IPv4 addressing is the default.

Command Modes

Multicast routing address-family configuration
Multicast VPN configuration

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.

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
The following example shows how to configure SSM service for the IP address range defined by access list 4, using the `ssm` command:

```plaintext
RP/0/RP0/CPU0:router(config)# ipv4 access-list 4
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 224.2.151.141
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# ssm range 4
```
ssm
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* in .

- mrinfo, on page 212
- mtrace, on page 214
- sap cache-timeout, on page 216
- sap listen, on page 217
- show sap, on page 218
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>host-address</td>
<td>Can be either the Domain Name System (DNS) name or IP address of a multicast router entered in A.B.C.D format.</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional) Source address used on multicast routing information (mrinfo) requests. If omitted, the source is based on the outbound interface for the destination.</td>
</tr>
</tbody>
</table>

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

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**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]
**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] source destination [group_addr] [resp_addr] [ttl]```

**Syntax Description**

- **source**: Domain Name System (DNS) name or the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.
- **destination**: DNS name or address of the unicast destination. This is a unicast address of the end of the path to be traced.
- **group_addr** (Optional): DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for MBONE Audio). When address 0.0.0.0 is used, the software invokes a weak mtrace. A weak mtrace is one that follows the Reverse Path Forwarding (RPF) path to the source, regardless of whether any router along the path has multicast routing table state.
- **resp_addr** (Optional): DNS name or multicast address of the querier address to receive response. If the querier is not reachable by the RP or the source, this value should be provided.
- **ttl** (Optional): Time-to-live (TTL) threshold for a multicast trace request. Range is 1 to 255 router hops.

**Command Default**

By default, this feature is disabled.
IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**.
### 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 172.16.1.0 172.16.1.10 239.254.254.254 45.244.244.244 49
```
sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the sap cache-timeout command in global configuration mode. To return to the default behavior, use the no form of this command.

```
sap cache-timeout minutes
no sap cache-timeout
```

**Syntax Description**

- **minutes**  Time that a SAP cache entry is active in the cache. Range is 1 to 1440.

**Command Default**

- **minutes** : 1440 (24 hours)

**Command Modes**

- Global configuration
- XR Config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
</tr>
<tr>
<td><strong>name</strong></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sap, on page 218</td>
<td>Displays the SAP sessions learned on the configured multicast groups.</td>
</tr>
</tbody>
</table>
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-addresssession-name}] [detail]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) Group IP address or name of the session that is learned.</td>
</tr>
<tr>
<td>session-name</td>
<td>(Optional) Session name.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Provides more SAP information.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show sap` command. Information is summarized and shows one entry.

```
RP/0/RP0/CP0:router# show sap

Sap Session Table Summary
Cisco Systems, Inc
```
This table describes the significant fields shown in the display.

**Table 30: show sap Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src</td>
<td>IP address of the host from which this session announcement was received.</td>
</tr>
<tr>
<td>Dst</td>
<td>Destination IP multicast group address where the announcement was sent.</td>
</tr>
<tr>
<td>Last Heard</td>
<td>Time (in hours, minutes, and seconds) when SAP announcements were last heard from the source.</td>
</tr>
<tr>
<td>Total Entries</td>
<td>Total number of entries displayed.</td>
</tr>
</tbody>
</table>

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# 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 31: show sap detail Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Name</td>
<td>Descriptive name of the SAP session.</td>
</tr>
<tr>
<td>Description</td>
<td>An expanded description of the session.</td>
</tr>
<tr>
<td>Group</td>
<td>IP multicast group addresses used for this session.</td>
</tr>
<tr>
<td>Announcement source</td>
<td>IP address of the host from which this session announcement was received.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination IP multicast group address that the announcement was sent to.</td>
</tr>
<tr>
<td>Created by</td>
<td>Information for identifying and tracking the session announcement.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Indicates attributes specific to the session.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
sap listen, on page 217 | Configures the SDR listener on a group IP address. |