IP Multicast Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

First Published: January 25, 2013

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

CONTENTS

C through ip igmp

clear ip cgmp

To clear all group entries from the caches of Catalyst switches, use the **clear ip cgmp** command in privileged EXEC mode.

clear ip cgmp [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sends a Cisco Group Management Protocol (CGMP) leave message with a group address of 0000.0000.0000 and a unicast address of 0000.0000.0000. This message instructs the switches to clear all group entries they have cached.

If an interface type and number are specified, the leave message is sent only on that interface. Otherwise, it is sent on all CGMP-enabled interfaces.

Examples

The following example clears the CGMP cache:

```
Router# clear ip cgmp
```

Related Commands

Command	Description
ip cgmp	Enables CGMP on an interface of a router connected to a Catalyst 5000 switch.

clear ip msdp peer

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

clear ip msdp[**vrf** *vrf-name*]**peer**{*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the TCP connection is cleared.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Examples

The following example shows how to clear the TCP connection to the MSDP peer at 10.3.32.154:

```
Router# clear ip msdp peer 10.3.32.154
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

clear ip msdp sa-cache

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

clear ip msdp [**vrf** *vrf-name*] **sa-cache** [*group-address*| *group-name*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	(Optional) Multicast group address or name for which SA entries are cleared from the SA cache.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In order to have any SA entries in the cache to clear, SA caching must have been enabled with the **ip msdp cache-sa-state** command.

If no multicast group is identified by group address or name, all SA cache entries are cleared.

Examples

The following example shows how to clear the SA entries for the multicast group 10.3.50.152 from the cache:

```
Router# clear ip msdp sa-cache 10.3.50.152
```

Related Commands

Command	Description
ip host	Configures an MSDP peer.
ip msdp cache-sa-state	Enables the router to create SA state.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

clear ip msdp statistics

To clear statistics counters for one or all of the Multicast Source Discovery Protocol (MSDP) peers without resetting the sessions, use the **clear ip msdp statistics** command in privileged EXEC mode.

clear ip msdp[**vrf** *vrf-name*]**statistics**{*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	(Optional) Address or name of the MSDP peers whose statistics counters, reset count, and input/output count are cleared.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to clear the counters for the peer named peer1:

```
Router# clear ip msdp statistics peer1
```

Related Commands

Command	Description
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

ip cgmp

To enable Cisco Group Management Protocol (CGMP) on an interface of a router connected to a Cisco Catalyst switch, use the ip cgmp command in interface configuration mode. To disable CGMP routing, use the no form of this command.

ip cgmp [**proxy**| **router-only**]

no ip cgmp

Syntax Description

proxy	(Optional) Enables CGMP and the CGMP proxy function.
router-only	(Optional) Enables the router to send only CGMP self-join and CGMP self-leave messages.

Command Default

CGMP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2	The **router-only** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When enabled on an interface, this command triggers a CGMP join message. This command should be used only on 802 media (that is, Ethernet, FDDI, or Token Ring) or ATM. When a no **ip cgmp** command is issued, a triggered CGMP leave message is sent for the MAC address on the interface for group 0000.0000.0000 (all groups). CGMP can run on an interface only if Protocol Independent Multicast (PIM) is configured on the same interface.

A Cisco router will send CGMP join messages in response to receiving Internet Group Management Protocol (IGMP) reports from IGMP-capable members. Only the CGMP querier Cisco router sends these CGMP join messages on behalf of hosts.

The **ip cgmp router-only** command enables the routers in a VLAN to send only CGMP self-join and CGMP self-leave messages--no other types of CGMP messages will be sent. This feature allows other CGMP-capable routers to learn about multicast router ports. If the **ip cgmp router-only** command is not available on any of the external routers in the network, the **ip cgmp** command can be used instead. Issuing the **ip cgmp** command on a router enables that router to send CGMP self-join and CGMP self-leave messages as well as other types of CGMP messages.

When the **proxy** keyword is specified, the CGMP proxy function is also enabled. That is, any router that is not CGMP-capable will be advertised by the proxy router. The proxy router advertises the existence of other non-CGMP-capable routers by sending a CGMP join message with the MAC address of the non-CGMP-capable router and a group address of 0000.0000.0000.

Initially supported is Distance Vector Multicast Routing Protocol (DVMRP) proxying. If a DVMRP report is received from a router that is not a PIM router, a Cisco IGMP querier will advertise the MAC address of the DVMRP router in a CGMP join message with the group address 0000.0000.0000.

To perform CGMP proxy, a Cisco router must be the IGMP querier. If you configure the **ip cgmp proxy** command, you must manipulate the IP addresses so that a Cisco router will be the IGMP querier, which might be the highest or lowest IP address, depending on which version of IGMP is being run on the network. An IGMP Version 2 querier is selected based on the lowest IP addressed router on the interface. An IGMP Version 1 querier is selected based on the multicast routing protocol used on the interface.

When multiple Cisco routers are connected to a switched network and the **ip cgmp proxy** command is needed, we recommend that all routers be configured in the following manner:

- With the same CGMP option.
- To have precedence of becoming IGMP querier over non-Cisco routers.

Examples

The following example enables CGMP:

```
ip cgmp
```

The following example enables CGMP and CGMP proxy:

```
ip cgmp proxy
```

ip igmp access-group

To restrict hosts (receivers) on a subnet to joining only multicast groups that are permitted by a standard IP access list or to restrict hosts (receivers) on a subnet to membership to only the (S,G) channels that are permitted by an extended IP access list, use the **ip igmp access-group** command in interface configuration mode. To disable this control, use the **no** form of this command.

ip igmp access-group *access-list*

no ip igmp access-group *access-list*

Syntax Description

access-list	Access list number or name.

Command Default

Disabled (no access lists are configured for receiver access control).

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	Extended access list support was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp access-group** command to filter groups from Internet Group Management Protocol (IGMP) reports by use of a standard access list or to filter sources and groups from IGMPv3 reports by use of an extended access list. This command is used to restrict hosts on a subnet to joining only multicast groups that are permitted by a standard IP access list or to restrict hosts on a subnet to membership to only those (S, G) channels that are permitted by an extended IP access list.

IGMP Version 3 (IGMPv3) accommodates extended access lists, which allow you to leverage an important advantage of Source Specific Multicast (SSM) in IPv4, that of basing access on source IP address. Prior to

this feature, an IGMP access list accepted only a standard access list, allowing membership reports to be filtered based only on multicast group addresses.

IGMPv3 allows multicast receivers not only to join to groups, but to groups including or excluding sources. For appropriate access control, it is therefore necessary to allow filtering of IGMPv3 messages not only by group addresses reported, but by group and source addresses. IGMP extended access lists introduce this functionality. Using SSM with an IGMP extended access list allows you to permit or deny source S and group G (S, G) in IGMPv3 reports, thereby filtering SSM traffic based on source address, group address, or both.

Source Addresses in IGMPv3 Reports for ASM Groups

Additionally, IGMP extended access lists can be used to permit or filter traffic based on (0.0.0.0, G); that is, (*, G), in IGMP reports that are non-SSM, such as Any Source Multicast (ASM).

Note The permit and deny statements equivalent to (*, G) are **permit host 0.0.0.0 host** *group-address* and **deny host 0.0.0.0 host group** *group-address*, respectively.

Filtering applies to IGMPv3 reports for both ASM and SSM groups, but it is most important for SSM groups because multicast routing ignores source addresses in IGMPv3 reports for ASM groups. Source addresses in IGMPv3 membership reports for ASM groups are stored in the IGMP cache (as displayed with the **show ip igmp membership** command), but PIM-based IP multicast routing considers only the ASM groups reported. Therefore, adding filtering for source addresses for ASM groups impacts only the IGMP cache for ASM groups.

How IGMP Checks an Extended Access List

When an IGMP extended access list is referenced in the **ip igmp access-group** command on an interface, the (S, G) pairs in the permit and deny statements of the extended access list are matched against the (S, G) pair of the IGMP reports received on the interface. The first part of the extended access list clause controls the source, and the second part of the extended access list clause controls the multicast group.

Specifically, if an IGMP report with (S1, S2...Sn, G) is received, first the group (0, G) is checked against the access list statements. If the group is denied, the entire IGMP report is denied. If the group is permitted, each individual (S, G) pair is checked against the access list. Denied sources are taken out of the IGMP report, thereby denying any sources that match the access list from sending to the group.

Note The convention (0, G) means (*, G), which is a wildcard source with a multicast group number.

Examples

The following example shows how to configure a standard access list to filter the groups that are available on an interface for receivers to join. In this example, Ethernet interface 1/3 is configured to restrict receivers from joining groups in the range 226.1.0.0 through 226.1.255.255. Receivers are permitted to join all other groups on Ethernet interface 1/3.

```
access-list 1 deny 226.1.0.0 0.0.255.255
access-list 1 permit any log
!
interface ethernet 1/3
 ip igmp access-group 1
```

Note Access lists are very flexible; there is a seemingly limitless combination of permit and deny statements one could use in an access list to filter multicast traffic. The examples in this section simply provide a few examples of how it can be done.

The following example shows how to deny all states for a group G. In this example, FastEthernet interface 0/0 is configured to filter all sources for SSM group 232.2.2.2 in IGMPv3 reports, which effectively denies this group.

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface FastEthernet0/0
 ip igmp access-group test1
!
```

The following example shows how to deny all states for a source S. In this example, Ethernet interface 1/1 is configured to filter all groups for source 10.2.1.32 in IGMPv3 reports, which effectively denies this source.

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface Ethernet1/1
 ip igmp access-group test2
```

The following example shows how to permit all states for a group G. In this example, Ethernet interface 1/1 is configured to accept all sources for SSM group 232.1.1.10 in IGMPv3 reports, which effectively accepts this group altogether.

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface Ethernet1/1
 ip igmp access-group test3
```

The following example shows how to permit all states for a source S. In this example, Ethernet interface 1/2 is configured to accept all groups for source 10.6.23.32 in IGMPv3 reports, which effectively accepts this source altogether.

```
!
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface Ethernet1/2
 ip igmp access-group test4
!
```

The following example shows how to filter a particular source S for a group G. In this example, Ethernet interface 0/3 is configured to filter source 232.2.2.2 for SSM group 232.2.30.30 in IGMPv3 reports.

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface Ethernet0/3
 ip igmp access-group test5
```

ip igmp helper-address

To cause the system to forward all Internet Group Management Protocol (IGMP) host reports and leave messages received on the interface to the specified IP address, use the **ip igmp helper-address**command in interface configuration mode. To disable such forwarding, use the **no** form of this command.

ip igmp helper-address *ip-address*

no ip igmp helper-address

Syntax Description

ip-address	IP address to which IGMP host reports and leave messages are forwarded . Specify the IP address of an interface on the central router.

Command Default

IGMP host reports and leave messages are not forwarded.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

This command and the **ip pim neighbor-filter** command together enable stub multicast routing. The IGMP host reports and leave messages are forwarded to the IP address specified. The reports are re-sent out the next hop interface toward the IP address, with the source address of that interface. This command enables a type of "dense-mode" join, allowing stub sites not participating in Protocol Independent Multicast (PIM) to indicate membership in IP multicast groups.

Examples

The following example enables stub multicast routing on Router A, which has an outgoing interface with IP address 10.0.0.1. Router B is a central router with an incoming interface with address 10.0.0.2. Access list 1 filters PIM messages from the source (stub Router A).

Examples

```
ip multicast-routing
 ip pim dense-mode
 ip igmp helper-address 10.0.0.2
```

Examples

```
ip multicast-routing
 ip pim dense-mode : or ip pim sparse-mode
 ip pim neighbor-filter 1
access-list 1 deny 10.0.0.1
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating in PIM (for example, to configure stub multicast routing).

ip igmp limit (global)

To configure a global limit on the number of multicast route (mroute) states created as a result of Internet Group Management Protocol (IGMP) membership reports (IGMP joins), use the **ip igmp limit** command in global configuration mode. To remove the limit imposed by the global IGMP state limiter, use the **no** form of this command.

ip igmp limit *number*

no ip igmp limit *number*

Syntax Description

number	Maximum number of IGMP membership reports that can be cached. The range is from 1 to 64000.

Command Default

A global IGMP state limiter is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure a global limit on the number of mroute states created as a result of IGMP membership reports (IGMP joins). When configured globally, the limit is referred to as a global IGMP state limiter. Membership reports exceeding the configured limits are not entered into the IGMP cache. This command can be used to prevent DoS attacks.

Note IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URL Rendezvous Directory (URD) membership reports on a global or per interface basis.

Use the **ip igmp limit** (interface)command to configure a per interface limit on the number mroute states created as a result of IGMP membership reports (IGMP joins).

Note When configuring IGMP state limiters, you can only configure one global limit on a router and one limit per interface.

The mechanics of IGMP state limiters are as follows:

- Each time a router receives an IGMP membership report for a particular group or channel, the Cisco IOS software checks to see if either the limit for the global IGMP state limiter or the limit for the per interface IGMP state limiter has been reached.
  - If only a global IGMP state limiter has been configured and the limit has not been reached, IGMP membership reports are honored. When the configured limit has been reached, subsequent IGMP membership reports are then ignored (dropped) and a warning message in one of the following formats is generated:

```
%IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on <interface
 type number> by host <ip address>
```

or

```
%IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address, group address)>
 on <interface type number> by host <ip address>
```

  - If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
  - If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.

- If a per interface IGMP state limiter has been configured using the **ip igmp limit** (interface) command, the Cisco IOS software also checks to see if an access control list (ACL) is specified (with the optional **except** keyword and *access-list* argument) to prevent groups or channels from being counted against the interface limit.
  - If an ACL has been configured and the group or channel in the IGMP membership report matches, then the state for the IGMP membership is counted against the global limit and not the interface limit.
  - If no ACL has been configured, the per interface IGMP state limiter accounts for all IGMP membership reports that do not exceed the configured limit.

Examples

The following example shows how to configure a global IGMP state limiter that limits the number of mroute states created as result of IGMP membership reports to 300:

```
ip igmp limit 300
```

Related Commands

Command	Description
ip igmp limit (interface)	Limits the number of mroute states created as a result of IGMP membership reports on a per interface basis.

Command	Description
show ip igmp groups	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp limit (interface)

To configure a per interface limit on the number of multicast route (mroute) states created as a result of Internet Group Management Protocol (IGMP) membership reports (IGMP joins), use the **ip igmp limit** command in interface configuration mode. To remove the limit imposed by a per interface IGMP state limiter, use the **no** form of this command.

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit *number* [**except** *access-list*]

Syntax Description

number	Maximum number of IGMP states allowed on a router or interface. The range is from 1 to 64000.
except *access-list*	(Optional) Prevent groups or channels from being counted against the interface limit. A standard or an extended access control list (ACL) can be specified for the *access-limit* argument. • A standard ACL can be used to define the (*, G) state to be excluded from the limit on an interface. • An extended ACLs can be used to define the (S, G) state to be excluded from the limit on an interface. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list.

Command Default

No per interface IGMP state limiters are configured.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use this command to configure per interface limits on the number mroute states created as a result of IGMP membership reports (IGMP joins). When configured on an interface, the limit is referred to as a *per interface IGMP state limiter* . Membership reports exceeding the configured limits for the interface are not entered into the IGMP cache. This command can be used to prevent DoS attacks or to provide a multicast Call Admission Control (CAC) mechanism in network environments where all the multicast flows roughly utilize the same amount of bandwidth.

Note IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URD membership reports on a global or per interface basis.

For the required *number* argument, specify a limit on the number of IGMP membership reports that can be cached for the specified interface. The range is from 1 to 64000.

Use the optional except access-list keyword and argument to prevent groups or channels from being counted against the interface limit. A standard or an extended ACL can be specified.

- • A standard ACL can be used to define the (*, G) state to be excluded from the limit on an interface.
  - An extended ACLs can be used to define the (S, G) state to be excluded from the limit on an interface. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list.

Use the **ip igmp limit** (global)command to configure a global limit on the number of mroute states created as a result of IGMP membership reports (IGMP joins).

Note When configuring IGMP state limiters, you can only configure one global limit on a router and one limit per interface.

The mechanics of IGMP state limiters are as follows:

- Each time a router receives an IGMP membership report for a particular group or channel, the Cisco IOS software checks to see if either the limit for the global IGMP state limiter or the limit for the per interface IGMP state limiter has been reached.
  - If only a global IGMP state limiter has been configured and the limit has not been reached, IGMP membership reports are honored. When the configured limit has been reached, subsequent IGMP

membership reports are then ignored (dropped) and a warning message in one of the following formats is generated:

```
%IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on <interface
 type number> by host <ip address>
```

or

```
%IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address, group address)>
 on <interface type number> by host <ip address>
```

- • If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
  - If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.
- If a per interface IGMP state limiter has been configured using the **ip igmp limit** (interface) command, the Cisco IOS software also checks to see if an ACL is specified (with the optional **except** keyword and *access-list* argument) to prevent groups or channels from being counted against the interface limit.
  - If an ACL has been configured and the group or channel in the IGMP membership report matches, then the state for the IGMP membership is counted against the global limit and not the interface limit.
  - If no ACL has been configured, the per interface IGMP state limiter accounts for all IGMP membership reports that do not exceed the configured limit.

Examples

The following example shows how configure a per interface limiter that limits the number of mroute states created as result of IGMP membership reports on Gigabit Ethernet interface 0/1 to 100:

```
interface GigabitEthernet 0/1
 ip igmp limit 100
```

Related Commands

Command	Description
ip igmp limit (global)	Globally limits the number of IGMP states resulting from IGMP membership reports (IGMP joins).
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp mroute-proxy

To enable Internet Group Management Protocol (IGMP) report forwarding of proxied (*, G) multicast static route (mroute) entries, use the **ip igmp mroute-proxy** command in interface configuration mode. To disable this service, use the **no** form of this command.

ip igmp mroute-proxy *interface-type interface-number*

no ip igmp mroute-proxy *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number.

Command Default

The command is disabled.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When used with the **ip igmp proxy-service** interface command, this command enables forwarding of IGMP reports to a proxy service interface for all (*, G) forwarding entries for this interface in the multicast forwarding table.

Examples

The following example shows how to configure the **ip igmp mroute-proxy** command on Ethernet interface 1 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Ethernet interface 1. This example also shows how to configure the **ip igmp proxy-service** command on loopback interface 0 to enable the forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command.

```
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
```

```
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface ethernet 0
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
```

Related Commands

Command	Description
ip igmp proxy-service	Enables the mroute proxy service.
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip igmp proxy-service

To enable the mroute proxy service, use the **ip igmp proxy-service** command in interface configuration mode. To disable forwarding, use the **no** form of this command.

ip igmp proxy-service

no ip igmp proxy-service

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Based on the Internet Group Management Protocol (IGMP) query interval, the router periodically checks the multicast static route (mroute) table for (*, G) forwarding entries that match interfaces configured with the **ip igmp mroute-proxy** command. Where there is a match, one IGMP report is created and received on this interface. The **ip igmp proxy-service**command is intended to be used with the **ip igmp helper-address (UDL)** command, in which case the IGMP report would be forwarded to an upstream router.

Examples

The following example shows how to configure the **ip igmp mroute-proxy** command on Ethernet interface 1 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Ethernet interface 1. This example also shows how to configure the **ip igmp proxy-service** command on loopback interface 0 to enable the forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command.

```
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
ip igmp helper-address udl ethernet 0
```

```
ip igmp proxy-service
!
interface ethernet 0
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
```

Related Commands

Command	Description
ip igmp helper-address (UDL)	Configures IGMP helpering as required for IGMP UDLR.
ip igmp mroute-proxy	Enables IGMP report forwarding of proxied (*, G) mroute entries.
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip igmp snooping

To enable Internet Group Management Protocol (IGMP) snooping globally or on an interface, use the **ip igmp snooping** command in the global configuration mode, interface configuration, or bridge domain configuration mode. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP snooping is enabled globally.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration mode.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all existing VLAN interfaces.

When IGMP snooping is globally disabled, IGMP snooping is disabled on all existing bridge domain interfaces. When IGMP snooping is globally enabled, IGMP snooping is enabled on all existing bridge domain interfaces unless IGMP snooping was also explicitly disabled on a specific bridge domain interface. When IGMP

snooping is disabled globally and on a specific bridge domain interface, globally enabling IGMP snooping will not enable snooping on the bridge domain interface; it must be explicitly re-enabled on the bridge domain interface.

Use the **show ip igmp snooping** privileged EXEC command to verify your IGMP settings.

The configuration is saved in NVRAM.

For Cisco 7600 series routers: Before you can enable IGMP snooping for Cisco 7600 series routers, you must configure the VLAN interface for multicast routing.

Examples

The following examples show how to globally disable IGMP snooping and how to disable IGMP snooping on a specified bridge domain interface:

```
Router(config)# no ip igmp snooping
Router(config)# exit
Router# show running-config
.
.
.
no ip igmp snooping
Router(config)# bridge-domain1
Router(config-bdomain)# no ip igmp snooping
Router(config-bdomain)# end
Router# show running-config
.
.
.
bridge-domain 1
 no ip igmp snooping
!
!
```

The following example shows how to globally enable IGMP snooping after it was explicitly disabled:

```
Router(config)# ip igmp snooping
```

Related Commands

Command	Description
ip igmp snooping fast-leave	Enables the IGMPv3-snooping fast-leave processing.
ip igmp snooping vlan	Enables IGMP snooping on a VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping last-member-query-interval

To configure the last member query interval for IGMP snooping, use the **ip igmp snooping last-member-query-interval** command in the interface configuration or bridge domain configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping last-member-query-interval *interval*

no ip igmp snooping last-member-query-interval

Syntax Description

interval	Length of time, in milliseconds, after which the group record is deleted if no reports are received. The default is 1000. See the "Usage Guidelines" section for more information. For interfaces, the range is from 100 to 999, in multiples of 100. If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds. For bridge domain interfaces, the range is from 100 to 32767.

Command Default

The default interval is 1000 milliseconds (1 second).

Command Modes

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration mode.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-count** command to specify how often an IGMP query is sent in response to receiving an IGMP leave message.

The *interval* is the actual time that the Cisco 7600 series router waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no igmp snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of 1000. If you want this value, you must enter the **no ip igmp snooping last-member-query-interval** command to return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)#
ip igmp snooping last-member-query-interval 200
```

Related Commands

Command	Description
ip igmp snooping fast-leave	Enables the IGMP v3-snooping fast-leave processing.
ip igmp snooping last-member-query-count	Configures the interval for snooping queries sent.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

ip igmp snooping report-suppression

To turn on IP IGMP snooping report suppression, use the **ip igmp snooping report-suppression** command in the global configuration, interface configuration, or bridge domain configuration mode. To turn off report suppression, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP snooping report supression is disabled.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration mode.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to enable report supression for all host reports responding to a general query or for all host reports on an interface or a bridge domain.

When you enable report suppression for all host reports responding to a general query, IP IGMP snooping forwards the first report only and suppresses the remaining reports to constrain IGMP traffic to the multicast router.

Examples

This example shows how to enable IP IGMP snooping report suppression:

```
Router(config-if)# ip igmp snooping report-suppression
```

This example shows how to disable IP IGMP snooping report suppression:

```
Router(config-bdomain)# no ip igmp snooping report-suppression
```

ip igmp snooping vlan

To enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN, use the **ip igmp snooping vlan**command in global configuration mode. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Syntax Description

vlan-id	VLAN ID value. The range is from 1 to 1001. Do not enter leading zeroes.

Command Default

By default, IGMP snooping is enabled when each VLAN is created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

This command automatically configures the VLAN if it is not already configured. The configuration is saved in NVRAM.

Examples

The following example shows how to enable IGMP snooping on VLAN 2:

```
Router(config)# ip igmp snooping vlan 2
```

The following example shows how to disable IGMP snooping on VLAN 2:

```
Router(config)# no
 ip igmp snooping vlan 2
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping vlan immediate-leave

To enable Internet Group Management Protocol (IGMP) Immediate-Leave processing on a VLAN interface, use the **ip igmp snooping vlan immediate-leave**command in global configuration mode. To disable Immediate-Leave processing on the VLAN interface, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Syntax Description

vlan-id	VLAN ID value. The range is between 1 to 1001. Do not enter leading zeroes.

Command Default

By default, IGMP Immediate-Leave processing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

Use Immediate-Leave processing only when there is only one IP multicast receiver present on every port in the VLAN. The Immediate-Leave configuration is saved in NVRAM.

Immediate-Leave processing is supported only with IGMP version 2 hosts.

Examples

The following example shows how to enable IGMP Immediate-Leave processing on VLAN 1:

```
Router(config)# ip igmp snooping vlan 1 immediate-leave
```

The following example shows how to disable IGMP Immediate-Leave processing on VLAN 1:

```
Router(config)# no
 ip igmp snooping vlan 1 immediate-leave
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

ip igmp snooping vlan mrouter

To add a multicast router port and to configure the multicast router learning method, use the **ip igmp snooping vlan mrouter**command in global configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id*| **learn pim-dvmrp**}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id*| **learn pim-dvmrp**}

Syntax Description

vlan-id	Specifies the VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
interface *interface-id*	Specifies the interface of the member port that is configured to a static router port.
learn pim-dvmrp	Specifies the multicast router snooping PIM-DVMRP packets multicast router learning method.

Command Default

The default learning method is **pim-dvmrp**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

The configured learning method is saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Examples

The following example shows how to configure Fast Ethernet interface 0/6 as a multicast router port:

```
Router(config)# ip igmp snooping vlan 1 mrouter interface fastethernet0/6
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping mrouter	Displays the statically and dynamically learned multicast router ports.

ip igmp snooping vlan static

To add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static**command in global configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **static** *mac-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *mac-address* **interface** *interface-id*

Syntax Description

vlan-id	Specifies the VLAN ID. The range is 1 to 1001. Do not enter leading zeroes.
mac-address	Specifies the static group MAC address.
interface *interface-id*	Specifies the interface configured to a static router port.

Command Default

No Layer 2 ports are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

This command is used to statically configure the IP multicast group member ports.

The static ports and groups are saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Use the **show mac-address-table multicast**privileged EXEC command to verify your Layer 2 multicast entries.

Examples

The following example shows how to statically configure a host on an interface:

```
Router(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface fastethernet0/6
Configuring port FastEthernet 0/6 on group 0100.5e02.0203
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

ip igmp static-group

To configure static group membership entries on an interface, use the **ip igmp static-group** command in interface configuration mode. To delete static group membership entries, use the **no** form of this command.

ip igmp static-group {*****| *group-address* [**source** {*source-address*| **ssm-map**}]| **class-map** *class-map-name*}

no ip igmp static-group {*****| *group-address* [**source** {*source-address*| **ssm-map**}]| **class-map** *class-map-name*}

Syntax Description

*****	Places the interface into all created multicast route (mroute) entries.
group-address	IP multicast group address to configure as a static group member on the interface.
source	(Optional) Statically forwards a (S, G) channel out of the interface.
source-address	(Optional) IP address of a system where multicast data packets originate.
ssm-map	(Optional) Configures Source Specific Multicast (SSM) mapping to be used on the interface to determine the source associated with this group. The resulting (S, G) channels are statically forwarded.
class-map *class-map-name*	Attaches an Internet Group Management Protocol (IGMP) static group range class map to the interface.

Command Default

No static group membership entries are configured on interfaces.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)T	This command was modified. The **ssm-map** keyword was added.
12.2(18)S	This command was modified. The **ssm-map** keyword was added.
12.2(18)SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF5	This command was modified. The **class-map** keyword and *class-map-name* argument were added.
15.0(1)M	This command was modified. The **class-map** keyword and *class-map-name* argument were added.
12.2(33)SRE	This command was modified. The **class-map** keyword and *class-map-name* argument were added.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **ip igmp static-group** command to configure static group membership entries on an interface. When you configure this command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface. Once configured, static group membership entries are added to the IGMP cache and mroute table.

Configuring the **ip igmp static-group** command is unlike configuring the **ip igmp join-group** command, which allows the router to join the multicast group. This configuration of the **ip igmp static-group** command would cause the upstream routers to maintain the multicast routing table information for that group, which would ensure that all the paths to that multicast group are active.

If you configure the **ip igmp join-group** command for the same group address as the **ip igmp static-group** command, the **ip igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Use the **ip igmp static-group** command with the **ssm-map** keyword to configure static traffic forwarding with SSM mapping on the last hop router. Static traffic forwarding can be used in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses Domain Name System (DNS)-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

Use the **ip igmp static-group class-map** command with the **class-map** keyword and *class-map-name* argument to attach an IGMP static group class map to an interface. Once attached, all groups entries that are defined in the class map become static members on the interface and are added to the IGMP cache and to the mroute table.

For Cisco IOS Release 15.1(1)T and later releases

The MFIB maintains a (*, G/m) entry that handles dense mode packets. When the first dense mode packet arrives on a router, it matches this (*, G/m) entry. The packet is punted to the route processor only if at least

one of the following two conditions is met: The source of the packet is directly connected to this router or the interface on which the packet was received has at least one PIM neighbor. If neither of these conditions is met, the (*, G/m) entry in the MFIB drops the packet without punting it. If the interface of a last hop router does not have any PIM neighbors and does not have a receiver, configure the **ip igmp static-group** command with the ***** keyword before any receiver joins (before any (*, G) state is created on the router) to simulate the presence of a receiver for all multicast group addresses on the interface, causing the interface to be added to the olist of the mroute entry and preventing incoming last hop router traffic for a dense mode group on the interface from being dropped.

Examples

The following example shows how to configure group address 239.100.100.101 on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.100.100.101
```

The following example shows how to configure group address 239.1.2.1 to use SSM mapping for statically forwarded groups on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.1.2.1 source ssm-map
```

The following example shows how to attach an IGMP static group range class map named static1 to GigabitEthernet interface 1/1:

```
interface GigabitEthernet1/1
 ip igmp static-group class-map static1
```

Related Commands

Command	Description
class-map type multicast-flows	Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps.
ip igmp join-group	Causes the router to join a multicast group.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip igmp ssm-map query dns	Configures DNS-based SSM mapping.
ip igmp ssm-map static	Enables static SSM mapping.
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp unidirectional-link

To configure an interface to be unidirectional and enable it for Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), use the **ip igmp unidirectional-link**command in interface configuration mode. To disable the unidirectional link (UDL), use the **no** form of this command.

ip igmp unidirectional-link

no ip igmp unidirectional-link

Syntax Description

This command has no arguments or keywords.

Command Default

No UDLR occurs.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

One example of when you might configure this command is if you have traffic traveling via a satellite.

If you have a small number of receivers, another way to achieve UDLR is to configure a UDLR tunnel. See the descriptions of the **tunnel udlr receive-only** and **tunnel udlr send-only** commands.

Examples

The following example configures an upstream router with UDLR on serial interface 0:

```
ip multicast-routing
!
! Unidirectional link
!
interface serial 0
 description Unidirectional to downlink-rtr
 ip address 10.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp unidirectional-link
 no keepalive
```

Related Commands

Command	Description
ip igmp helper-address (UDL)	Configures IGMP helpering as required for IGMP UDLR.
ip igmp mroute-proxy	Enables IGMP report forwarding of proxied (*, G) mroute entries.
ip igmp proxy-service	Enables the mroute proxy service.
ip multicast default-rpf-distance	Changes the distance given to the default RPF interface when configuring IGMP UDLR.
show ip igmp udlr	Displays UDLR information for directly connected multicast groups on interfaces that have a UDL helper address configured.
tunnel udlr receive-only	Configures a unidirectional, GRE tunnel to act as a back channel that can receive messages, when another interface is configured for UDLR to send messages.
tunnel udlr send-only	Configures a unidirectional, GRE tunnel to act as a back channel that can send messages, when another interface is configured for UDLR to receive messages.

ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version**command in interface configuration mode. To restore the default value, use the **no** form of this command.

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

no ip igmp version

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2. This is the default.
3	IGMP Version 3.

Command Default

Version 2

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)T	The **3**keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This Bandwidth-Based Call Admission Control for IP Multicast command was modified. Support was added for this command in virtual network interface configuration mode.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

All routers on the subnet must support the same version. The router does not automatically detect Version 1 routers and switch to Version 1 as did earlier releases of the Cisco IOS software. Hosts can have any IGMP version (1, 2, or 3) and the router will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2 or 3, such as the **ip igmp query-max-response-time**and **ip igmp query-timeout**commands.

Examples

The following example configures the router to use IGMP Version 3:

```
ip igmp version 3
```

Related Commands

Command	Description
ip igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp query-timeout	Configures the timeout time before the router takes over as the querier for the interface, after the previous querier has stopped querying.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.

ip msdp through M

ip msdp default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **ip msdp default-peer**command in global configuration mode. To remove the default peer, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*]**default-peer**{*peer-address*| *peer-name*}[**prefix-list** *list*]

no ip msdp [**vrf** *vrf-name*] **default-peer**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address *peer-name*	IP address or Domain Name System (DNS) name of the MSDP default peer.
prefix-list *list*	(Optional) Specifies the Border Gateway Protocol (BGP) prefix list that specifies that the peer will be a default peer only for the prefixes listed in the list specified by the *list* argument. A BGP prefix list must be configured for this **prefix-list** *list* keyword and argument to have any effect.

Command Default

No default MSDP peer exists.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

If only one MSDP peer is configured (with the **ip msdp peer** command), it will be used as a default peer. Therefore, you need not configure a default peer with this command.

If 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 if you intend to configure the **prefix-list** *list* keyword and argument with the **ip msdp default-peer**command.

If the **prefix-list** *list* keyword and argument are specified, SA messages originated from rendezvous points (RPs) specified by the **prefix-list** *list* keyword and argument will be accepted from the configured default peer. If the **prefix-list** *list* keyword and argument are specified but no prefix list is configured, the default peer will be used for all prefixes.

You can enter multiple **ip msdp default-peer**commands, with or without the **prefix-list** keyword, as follows. However, all commands must either have the keyword or all must not have the keyword.

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

Examples

The following example shows how to configure the router at IP address 192.168.1.3 as the default peer to the local router:

```
ip msdp peer 192.168.1.3
ip msdp peer 192.168.3.5
ip msdp default-peer 192.168.1.3
```

The following example shows how to configure two default peers:

```
ip msdp peer 172.18.2.3
ip msdp peer 172.19.3.5
ip msdp default-peer 172.18.2.3 prefix-list site-c
ip prefix-list site-a permit 172.18.0.0/16
ip msdp default-peer 172.19.3.5 prefix-list site-a
ip prefix-list site-c permit 172.19.0.0/16
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip prefix-list	Creates a prefix list.

ip msdp description

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

ip msdp [**vrf** *vrf-name*] **description** {*peer-name*| *peer-address*} *text*

no ip msdp [**vrf** *vrf-name*] **description** {*peer-name*| *peer-address*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name *peer-address*	Peer name or address to which this description applies.
text	Description of the MSDP peer.

Command Default

No description is associated with an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Examples

The following example shows how to configure the router at the IP address 172.17.1.2 with a description indicating it is a router at customer A:

```
ip msdp description 172.17.1.2 router at customer a
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about the MSDP peer.

ip msdp filter-sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request**command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address*| *peer-name*} [**list** *access-list*]

no ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.
list *access-list*	(Optional) Specifies the standard IP access list number or name that describes a multicast group address. If no access list is specified, all SA request messages are ignored.

Command Default

By default, the router honors all SA request messages from peers. If this command is not configured, all SA request messages are honored. If this command is configured but no access list is specified, all SA request messages are ignored.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, the router honors all SA request messages from peers. Use this command if you want to control exactly which SA request messages the router will honor.

If no access list is specified, all SA request messages are ignored. If an access list is specified, only SA request messages from those groups permitted will be honored, and all others will be ignored.

Examples

The following example shows how to configure the router to filter SA request messages from the MSDP peer at 172.16.2.2. SA request messages from sources on the network 192.168.22.0 pass access list 1 and will be honored; all others will be ignored.

```
ip msdp filter-sa-request 172.16.2.2 list 1
access-list 1 permit 192.4.22.0 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp mesh-group

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **ip msdp mesh-group**command in global configuration mode. To remove an MSDP peer from a mesh group, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address*| *peer-name*}

no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mesh-name	Name of the mesh group.
peer-address | *peer-name*	IP address or name of the MSDP peer to be a member of the mesh group.

Command Default

The MSDP peers do not belong to a mesh group.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. 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 achieve two goals:

- To reduce SA message flooding
- To simplify peer-Reverse Path Forwarding (RPF) flooding (no need to run Border Gateway Protocol [BGP] or multiprotocol BGP among MSDP peers)

Examples

The following example shows how to configure the MSDP peer at address 192.168.1.3 to be a member of the mesh group named internal:

```
ip msdp mesh-group internal 192.168.1.3
```

ip msdp peer

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp peer** command in global configuration mode. To remove the peer relationship, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **peer** {*peer-name*| *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]

no ip msdp [**vrf** *vrf-name*] **peer** {*peer-name*| *peer-address*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name *peer-address*	Domain Name System (DNS) name or IP address of the router that is to be the MSDP peer.
connect-source *interface-type interface-number*	(Optional) Specifies the interface type and number whose primary address becomes the source IP address for the TCP connection. This interface is on the router being configured.
remote-as *as-number*	(Optional) Specifies the autonomous system number of the MSDP peer. This keyword and argument are used for display purposes only.

Command Default

No MSDP peer is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The router specified should also be configured as a BGP neighbor.

The *interface-type* is on the router being configured.

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

The **remote-as** *as-number*keyword and argument are used for display purposes only.

A peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it displays as the autonomous system number of the peer.

Examples

The following example shows how to configure the router at the IP address 192.168.1.2 as an MSDP peer to the local router. The neighbor belongs to autonomous system 109.

```
ip msdp peer 192.168.1.2 connect-source ethernet 0/0
router bgp 110
 network 192.168.0.0
 neighbor 192.168.1.2 remote-as 109
 neighbor 192.168.1.2 update-source ethernet 0/0
```

The following example shows how to configure the router at the IP address 192.168.1.3 as an MSDP peer to the local router:

```
ip msdp peer 192.168.1.3
```

The following example shows how to configure the router at the IP address 192.168.1.4 to be an MSDP peer in autonomous system 109. The primary address of Ethernet interface 0/0 is used as the source address for the TCP connection.

```
ip msdp peer 192.168.1.4 connect-source ethernet 0/0 remote-as 109
```

Related Commands

Command	Description
ip msdp default-peer	Defines a default peer from which to accept all MSDP SA messages.
neighbor remote-as	Adds an entry to the BGP neighbor table.

ip msdp sa-filter out

To configure an outgoing filter list for Source-Active (SA) messages sent to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter out**command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp[**vrf** *vrf-name*]**sa-filter out** {*peer-address*| *peer-name*}[**list** *access-list-name*][**route-map** *map-name*][**rp-list**{*access-list-range*| *access-list-name*}][**rp-route-map** *route-map reference*]

no ip msdp[**vrf** *vrf-name*]**sa-filter out** {*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer to which the SA messages are filtered.
list *access-list-name*	(Optional) Specifies the IP access list to pass certain source and group pairs.
route-map *map-name*	(Optional) Specifies the route map match criteria for passing certain source and group pairs.
rp-list	(Optional) Specifies an access list for an originating Route Processor.
access-list range	Number assigned to an access list. The range is from 1 to 99.
access-list name	Name assigned to an access list.
rp-route-map *route-map reference*	(Optional) Specifies the route map and route reference for passsing through a route processor.

Command Default

No outgoing messages are filtered; all SA messages received are forwarded to the peer.

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)T	This command was introduced.

Release	Modification
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was modified. Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **rp-list** keyword was added.

Usage Guidelines

If you use the **ip msdp sa-filter out** command without specifying access list name or route map match criteria, all source and group pairs from the peer are filtered. If you do specify an access-list name, the specified MSDP peer passes only those SA messages that pass the extended access list.

If you use the **route-map** *map-name* keyword and argument pair, the specified MSDP peer passes only those SA messages that meet the match criteria.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any source and group pairs in outgoing SA messages.

If all match criteria are true, a **permit** keyword from the route map will pass routes through the filter. A **deny** keyword will filter routes.

Examples

The following example shows how to permit only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer at the IP address 192.168.1.5:

```
Router> enable
Router# configure terminal
Router(config)# ip msdp peer 192.168.1.5 connect-source ethernet 0/0
Router(config)# ip msdp sa-filter out 192.168.1.5 list 100
Router(config)# access-list 100 permit ip 172.1.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.

ip msdp sa-limit

To limit the number of Source Active (SA) messages that can be added to the SA cache from a specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-limit** command in global configuration mode. To remove the limit imposed by the MSDP SA limiter, use the **no** form of this command.

ip msdp[**vrf** *vrf-name*]**sa-limit** {*peer-address*| *peer-name*}[*sa-limit*]

no ip msdp[**vrf** *vrf-name*]**sa-limit** {*peer-address*| *peer-name*}[*sa-limit*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the MSDP SA limiter be applied to the MSDP peer associated with Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-name *peer-address*	Domain Name System (DNS) name or IP address of the MSDP peer for which to apply the MSDP SA limiter.
sa-limit	Maximum number of SA messages that can be accepted (cached) from the specified peer. The range is from 1 to 2147483646.

Command Default

No MSDP SA limiters are configured for MSDP peers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(3)	This command was integrated into Cisco IOS Release 12.2(3).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure MSDP SA limiters, which impose limits on the number of MSDP SA messages that an MSDP-enabled router can accept (can be cached) from an MSDP peer. This command provides a means to protect an MSDP-enabled router from denial of service (DoS) attacks.

Mechanics of MSDP SA Limiters

- When MSDP SA limiters are configured, the router maintains a per-peer count of SA messages stored in the SA cache.
- SA messages that exceed the limit configured for an MSDP peer are ignored.
- If the router receives SA messages in excess of the configured limit from an MSDP peer, a warning in the following format is generated (once a minute) until the cache is cleared:

```
%MSDP-4-SA_LIMIT: SA from peer <peer address or name>, RP <RP address> for <mroute> exceeded
 sa-limit of <configured SA limit for MSDP peer>
```

Tips for Configuring MSDP SA Limiters

- We recommended that you configure MSDP SA limiters for all MSDP peerings on the router.
- An appropriately low MSDP SA limit should be configured on peerings with a stub MSDP region (an MSDP peer that may have some further downstream peers but does not act as a transit for SA messages across the rest of the Internet).
- An appropriately high SA limit should be configured for all MSDP peerings that act as transits for MSDP SA messages across the Internet.

The output of the **show ip msdp count**, **show ip msdp peer**, and **show ip msdp summary**commands will display the number of SA messages from each MSDP peer that is in the SA cache. If the **ip msdp sa-limit** command is configured, the output of the **show ip msdp peer** command will also display the value of the SA message limit for each MSDP peer.

Examples

The following example shows how to configure an MSDP SA limiter. In this example, an MSDP SA limiter is configured that imposes a limit of 100 SA messages from the MSDP peer at 192.168.10.1.

```
ip msdp sa-limit 192.168.10.1 100
```

Related Commands

Command	Description
show ip msdp count	Displays the number of sources and groups originated in MSDP SA messages.

Command	Description
show ip msdp peer	Displays detailed information about the MSDP peer.
show ip msdp summary	Displays MSDP peer status.

ip msdp sa-request

Note Effective with Cisco IOS Release 12.0(27)S, 12.2(20)S, 12.2(18)SXE, and 12.3(4)T, the **ip msdp sa-request** is not available in Cisco IOS software.

To configure the router to send Source-Active (SA) request messages to an Multicast Source Discovery Protocol (MSDP) peer when a new joiner from the group becomes active, use the **ip msdp sa-request**command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address*| *peer-name*}

no ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.

Command Default

The router does not send SA request messages to the MSDP peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.0(27)S	This command was removed from Cisco IOS Release 12.0(27)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S	This command was removed from Cisco IOS Release 12.2(20)S.
12.2(18)SXE	This command was removed from Cisco IOS Release 12.2(18)SXE.

Release	Modification
12.3(4)T	This command was removed from Cisco IOS Release 12.3(4)T.

Usage Guidelines

By default, the router does not send any SA request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive any SA messages that eventually arrive.

Use this command if you want a new member of a group to learn the current, active multicast sources in a connected Protocol Independent Multicast sparse mode (PIM-SM) domain that are sending to a group. The router will send SA request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its SA cache. If the peer does not have a cache configured, this command provides nothing.

An alternative to this command is using the **ip msdp cache-sa-state** command to have the router cache messages.

Examples

The following example shows how to configure the router to send SA request messages to the MSDP peer at the IP address 192.168.10.1:

```
ip msdp sa-request 192.168.10.1
```

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.
ip msdp peer	Configures an MSDP peer.

ip msdp shutdown

To administratively shut down a configured Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp shutdown**command in global configuration mode. To bring the peer back up, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address*| *peer-name*}

no ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address*| *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to shut down.

Command Default

No action is taken to shut down an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to shut down the MSDP peer at IP address 192.168.7.20:

```
ip msdp shutdown 192.168.7.20
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip multicast boundary

To configure an administratively scoped IPv4 multicast boundary, use the **ip multicast boundary**command in interface configuration mode. To remove the boundary, use the **no** form of this command.

ip multicast boundary *access-list* **[filter-autorp]**

no ip multicast boundary *access-list* **[filter-autorp]**

Cisco IOS 12.3(11)T and Subsequent T and Mainline Releases

ip multicast boundary *access-list* [**filter-autorp**| **in**| **out**]

no ip multicast boundary *access-list* [**filter-autorp**| **in**| **out**]

Cisco IOS XE Release 3.2S and Later Releases

no ip multicast boundary

Syntax Description

access-list	Number or name identifying an access control list (ACL) that controls the range of group addresses or (S, G) traffic affected by the boundary.
filter-autorp	(Optional) Filters auto-rendezvous point (Auto-RP) messages denied by the boundary ACL.
in	(Optional) Filters source traffic coming into the interface that is denied by the boundary ACL.
out	(Optional) Prevents multicast route (mroute) states from being created on an interface by filtering Protocol Independent Multicast (PIM) joins and Internet Group Management Protocol (IGMP) reports for groups or channels that are denied by the boundary ACL.

Command Default

No user-defined boundaries are configured.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.

Release	Modification
12.0(22)S	The **filter-autorp** keyword was added.
12.1(12c)E	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.1(12c)E.
12.2(11)	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(11).
12.2(13)T	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	The **in** and **out** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode. The *access-list* argument and **filter-autorp** keyword are no longer required with the **no**form of this command to remove the boundary ACL configuration.

Usage Guidelines

Use the **ip multicast boundary** command to configure an administratively scoped (user-defined) boundary on an interface in order to filter source traffic coming into the interface and prevent mroute states from being created on the interface.

Note An IP multicast boundary enables reuse of the same multicast group address in different administrative domains.

A standard ACL is used with the **ip multicast boundary**command to define the group address range to be permitted or denied on an interface. An extended ACL is used with the **ip multicast boundary** to define (S, G) traffic to be permitted or denied on an interface. Extended ACLs can also be used to define the (*, G) state to be permitted or denied on an interface, by specifying **host 0.0.0.0** for the source address in the permit statements that compose the extended ACL.

When you configure IP multicast boundaries for (S, G) traffic in an Any Source Multicast (ASM) network environment--to ensure that the IP multicast boundaries function properly--you must configure an extended ACL on routers along the rendezvous point tree (RPT) that permits:

- (S, G) traffic by specifying the source and group address range in permit statements.
- (*, G) traffic by specifying **host 0.0.0.0** for the source address followed by the group address or group address range in permit statements.
- Traffic destined to the rendezvous point (RP) by including permit statements for (RP, G), where the IP address of the RP is specified for the source followed by the group address or group address range.

The IP multicast boundary guideline for ASM applies only to the routers on the RPT from the last-hop router to the RP. For routers on the RP-to-source branch, you need to define only the (S, G) traffic in the extended ACL (by specifying the source and group address range in permit statements).

When you configure IP multicast boundaries for (S, G) traffic in a Source Specific Multicast (SSM) network environment, you need to define only the (S, G) traffic to be permitted or denied on an interface in the extended ACL.

IP multicast boundaries filter data and control plane traffic including IGMP, PIM Join and Prune, and Auto-RP messages. The following messages are not filtered by IP multicast boundaries:

- PIM Register messages are sent using multicast and not filtered.
- PIM Hellos for neighbor-ship to 224.0.0.13 are not filtered.
- Link local messages are not affected and PIM hellos on the local segment are not filtered. To disallow PIM adjacency formation on each link, use the **ip pim neighbor-filter** command in the interface or virtual network interface configuration mode.

If you configure the **filter-autorp** keyword, the user-defined boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Note Extended ACLs cannot be used with the **filter-autorp** keyword because Auto-RP announcements do not contain source addresses.

In Cisco IOS software releases that do not support the **in** and **out** keywords, the IP multicast boundary both filters source traffic coming into the interface and prevents mroute states from being created on the interface.

In Cisco IOS releases that support the **in** and **out** keywords, these keywords are used as follows:

- The **in** keyword is used to filter source traffic coming into the interface.
- The **out** keyword is used to prevent mroute states from being created on an interface; that is, it will prevent IGMP reports and PIM joins from creating mroutes states for groups and channels denied by the boundary ACL, and the interface will not be included in the outgoing interface list (OIL).
- If a direction is not specified with the **ip multicast boundary** command, the IP multicast boundary both filters source traffic coming into the interface and prevents mroute states from being created on the interface.

In addition, the following rules govern the use of the **in**, **out**, and **filter-autorp** keywords with the **ip multicast boundary** command:

- The **in** and **out** keywords support standard or extended ACLs for (S, G) filtering.
- The **in** and **out** keywords support standard or extended ACLs for SSM filtering.
- One instance of the **in** and **out** keywords can be configured on an interface.
- Only standard ACLs are permitted with the use of the **filter-autorp** keyword.

In Cisco 7600 series routers:

- A deny any statement at the end of the boundary ACL will cause all multicast boundaries including the link local address in the range (224.0.0.0 - 224.0.0.255) to be dropped in the hardware.
- When the ip multicast boundary *access-list* [**filter-autorp**] command is configured with an empty ACL, it interferes in the proper functioning of Auto-RP in the hardware. Hence, it is important to specify the address you want to allow or deny in the access-list.

In Cisco IOS XE Release 3.2S and later releases, the *access-list* and **filter-autorp**argument and keyword are no longer required with the **no** form of this command.

In Cisco IOS XE Release 3.1S and earlier releases, the **no ip multicast boundary** command must be configured with the ACL and the **filter-autorp** keyword to remove the boundary ACL configuration.

A maximum of three instances of an **ip multicast boundary** command is allowed on an interface: one instance of the command with the **in** keyword, one instance of the command with the **out**keyword, and one instance of the command with or without the **filter-autorp**keyword.

Examples

The following example shows how to set up an IP multicast boundary for all user-defined IPv4 multicast addresses by denying the entire user-defined IPv4 multicast address space (239.0.0.0/8). All other Class D addresses are permitted (224.0.0.0/4).

```
access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
interface ethernet 0
 ip multicast boundary 1
```

The following example shows how to set up an IP multicast boundary in an SSM network environment. In this example, the IP multicast boundary is configured to permit mroute states for (172.16.2.201, 232.1.1.1) and (172.16.2.202, 232.1.1.1). All other (S, G) traffic is implicitly denied.

```
ip access-list extended acc_grp1
permit ip host 172.16.2.201 host 232.1.1.1
permit ip host 172.16.2.202 host 232.1.1.1
interface ethernet 2/3
 ip multicast boundary acc_grp1 out
```

The following example shows how to configure an IP multicast boundary in an ASM network environment. In this example, the IP multicast boundary configuration on the last-hop router is shown. The topology for this example is not illustrated; however, assume that the IP address of the RP in this scenario is 10.1.255.104. The IP multicast boundary is configured to filter outgoing IP multicast traffic on Fast Ethernet interface 0/0. The boundary ACL used for the IP multicast boundary in this scenario contains three permit statements:

- The first permit statement specifies the (S, G) traffic to be permitted.
- The second permit statement specifies the (RP, G) traffic to be permitted.
- The third permit statement specifies the (*, G) traffic to be permitted.

All other outgoing multicast traffic on this interface is implicitly denied.

```
ip access-list extended bndry-asm-3
 permit ip host 10.1.248.120 239.255.0.0 0.0.255.255
 permit ip host 10.1.255.104 239.255.0.0 0.0.255.255
 permit ip host 0.0.0.0 239.255.0.0 0.0.255.255
interface FastEthernet0/0
 ip multicast boundary bndry-asm-3 out
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating in Protocol Independent Multicast (PIM).

ip multicast multipath

To enable load splitting of IP multicast traffic over Equal Cost Multipath (ECMP), use the **ip multicast multipath**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash** {**basic**| **next-hop-based**}]

no ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash** {**basic**| **next-hop-based**}]

Syntax Description

vrf *vrf-name*	(Optional) Enables ECMP multicast load splitting for IP multicast traffic associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
s-g-hash	(Optional) Enables ECMP multicast load splitting based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords: • **basic** --Enables a simple hash based on source and group address. This algorithm is referred to as the basic S-G-hash algorithm. • **next-hop-based** --Enables a more complex hash based on source, group, and next-hop address. This algorithm is referred to as the next-hop-based S-G-hash algorithm.

Command Default

If multiple equal-cost paths exist, multicast traffic will not be load split across those paths.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.

Release	Modification
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name*argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **s-g-hash**, **basic**, and **next-hop-based** keywords were added in support of the IP Multicast Load Splitting--Equal Cost Multipath (ECMP) Using S, G and Next Hop feature.
15.0(1)M	This command was modified. The **s-g-hash**, **basic**, and **next-hop-based** keywords were added in support of the IP Multicast Load Splitting--Equal Cost Multipath (ECMP) Using S, G and Next Hop feature.
15.0(1)S	This command was integrated into Cisco IOS Release15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **ip multicast multipath** command to enable load splitting of IP multicast traffic across multiple equal-cost paths.

If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.

Configuring load splitting with the **ip multicast multipath** command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.

Note The **ip multicast multipath**command load splits the traffic but does not *load balance* the traffic. Traffic from a source will use only one path, even if the traffic far outweighs traffic from other sources.

If the **ip multicast multipath** command is configured with the **s-g-hash** keyword and multiple equal-cost paths exist, load splitting will occur across equal-cost paths based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords:

- **basic** --Enables a simple hash based on source and group address. The basic S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. The basic S-G-hash algorithm, however, is subject to polarization because for a given source and group, the same hash is always picked irrespective of the router the hash is being calculated on.
- **next-hop-based** --Enables a more complex hash based on source, group, and next-hop address. The next-hop-based S-G-hash algorithm is predictable because no randomization is used in coming up with the hash value. Unlike the S-hash and basic S-G-hash algorithms, the next-hop-based hash mechanism is not subject to polarization.

Examples

The following example shows how to enable ECMP multicast load splitting on a router based on source address using the S-hash algorithm:

```
ip multicast multipath
```

The following example shows how to enable ECMP multicast load splitting on a router based on source and group address using the basic S-G-hash algorithm:

```
ip multicast multipath s-g-hash basic
```

The following example shows how to enable ECMP multicast load splitting on a router based on source, group, and next-hop address using the next-hop-based S-G-hash algorithm:

```
ip multicast multipath s-g-hash next-hop-based
```

ip multicast rpf backoff

To configure the intervals at which Protocol Independent Multicast (PIM) Reverse Path Forwarding (RPF) failover will be triggered by changes in the routing tables, use the ip multicast rpf backoff command in global configuration mode. To set the triggered RPF check to the default values, use the no form of this command.

ip multicast rpf backoff *minimum maximum* **[disable]**

no ip multicast rpf backoff *minimum maximum* **[disable]**

Syntax Description

minimum	The minimum configured backoff interval. The backoff interval is reset to the number of milliseconds (ms) configured by the *minimum* argument if a backoff interval has expired without any routing changes. The default is 500 milliseconds (ms).
maximum	The maximum amount of time, in milliseconds, allowed for a backoff interval. The maximum length of time that is allowed is 5000 ms. The default is 5000 ms.
disable	(Optional) Turns off the triggered RPF check function.

Command Default

This command is enabled by default.*minimum*: 500 ms.*maximum*: 5000 ms.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In an unstable unicast routing environment that uses triggered RPF checks, the environment could be constantly triggering RPF checks, which places a burden on the resources of the router. To avoid this problem, use the **ip multicast rpf backoff** command to prevent a second triggered RPF check from occurring for the length of time configured. That is, the PIM "backs off" from another triggered RPF check for a minimum amount of milliseconds as configured by the user.

If the backoff period expires without further routing table changes, PIM then scans for routing changes and accordingly establishes multicast RPF changes. However, if more routing changes occur during the backoff period, PIM doubles the backoff period to avoid overloading the router with PIM RPF changes while the routing table is still converging.

Note We recommend that users keep the default values for this command. The default values allow subsecond RPF failover.

The *maximum* argument is used to configure the maximum backoff interval. The backoff time is reset to the time configured by the *minimum* argument if an entire backoff interval has expired without routing changes.

The *maximum* argument default allows the RPF change behavior to be backward-compatible, allowing a 5-second RPF check interval in case of frequent route changes and a 500-ms RPF check interval in stable networks with only unplanned routing changes. Before the introduction of the **ip multicast rpf backoff** command, PIM polled the routing tables for changes every 5 seconds.

You likely need not change the defaults of the **ip multicast rpf backoff**command unless you have frequent route changes in your router (for example, on a dial-in router). Changing the defaults can allow you to reduce the maximum RPF check interval for faster availability of IP multicast on newly established routes or to increase the maximum RPF check interval to reduce the CPU load caused by the RPF check.

Examples

The following example shows how to set the minimum backoff interval to 100 ms and the maximum backoff interval to 2500 ms:

```
ip multicast rpf backoff 100 2500
```

ip multicast rpf interval

To modify the intervals at which periodic Reverse Path Forwarding (RPF) checks occur, use the **ip multicast rpf interval** command in global configuration mode. To return to the default interval, use the no form of this command.

ip multicast rpf interval *seconds* [**list** *access-list*| **route-map** *route-map*]

no ip multicast rpf interval *seconds* [**list** *access-list*| **route-map** *route-map*]

Syntax Description

seconds	The number of seconds at which the interval is configured. The default is 10 seconds.
list *access-list*	(Optional) Defines the interval of periodic RPF checks for an access list.
route-map *route-map*	(Optional) Defines the interval of periodic RPF checks for a route map.

Command Default

This command is enabled by default.*seconds*: 10

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can configure multiple instances of this command by using an access list or a route map.

Note We recommend that users keep the default values for this command. The default values allow subsecond RPF failover.

Examples

The following example shows how to set the periodic RPF check interval to 10 seconds:

```
ip multicast rpf interval 10
```

The following example shows how to set the periodic RPF check interval for groups that are defined by access list 10 to 3 seconds:

```
ip multicast rpf interval 3 list 10
```

The following example shows how to set the periodic RPF check interval for groups that are defined by the route map named map to 2 seconds:

```
ip multicast rpf interval 2 route-map map
```

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host hello messages.

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing**command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**vrf** *vrf-name*] **[distributed]**

no ip multicast-routing [**vrf** *vrf-name*]

Cisco IOS XE Release 3.3S

ip multicast-routing [**vrf** *vrf-name*] **distributed**

no ip multicast-routing [**vrf** *vrf-name*] **distributed**

Syntax Description

vrf *vrf-name*	(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
distributed	(Optional) Enables Multicast Distributed Switching (MDS).

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the **no** form of this command now disables IP multicast routing on the Multicast MultiLayer Switching (MMLS) Route Processor (RP) and purges all multicast MLS cache entries on the MMLS-SE.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S. This command without the **distributed** keyword was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	This command was modified. Either the **distributed** keyword or the **vrf** *vrf-name* **distributed** keyword and argument combination is required with this command in Cisco IOS Release 3.3S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T. The **distributed** keyword is not supported in Cisco IOS Release 15.2(3)T.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

The optional **distributed** keyword for this command is not supported in Cisco IOS XE Release 3.2S.

Either the **distributed** keyword or the **vrf** *vrf-name* **distributed** keyword and argument combination for this command is required in Cisco IOS XE Release 3.3S and later releases.

Note For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

Examples

The following example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)#
ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Router(config)#
no ip multicast-routing
```

The following example shows how to enable MDS in Cisco IOS XE Release 3.3S a specific VRF:

```
Router(config)#
ip multicast-routing vrf vrf1 distributed
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration or virtual network interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

ip pim {**dense-mode** [**proxy-register** {**list** *access-list*| **route-map** *map-name*}]| **passive**| **sparse-mode**| **sparse-dense-mode**}

no ip pim {**dense-mode** [**proxy-register** {**list** *access-list*| **route-map** *map-name*}]| **passive**| **sparse-mode**| **sparse-dense-mode**}

Syntax Description

dense-mode	Enables dense mode of operation.
proxy-register	(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR.
list *access-list*	(Optional) Defines an extended access list number or name.
route-map *map-name*	(Optional) Defines a route map.
passive	Enables passive mode of operation.
sparse-mode	Enables sparse mode of operation.
sparse-dense-mode	Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.

Command Default

PIM is disabled on all interfaces.

Command Modes

Interface configuration (config-if) Virtual network interface configuration (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
11.1	This command was modified. The **sparse-dense-mode**keyword was added.

Release	Modification
12.0S	This command was modified. The following keywords and arguments were added: • **proxy-register** • **list** *access-list* • **route-map** *map-name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **passive** keyword was added.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, passive mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets that it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface.

In Cisco IOS XE Release 3.2S and later releases, when PIM is enabled on an interface but the **ip multicast-routing** command has not been configured, a warning message, informing the user that the **ip multicast-routing** command is not configured and that multicast packets will not be forwarded, is no longer displayed.

Dense Mode

Initially, a dense mode interface forwards multicast packets until the router determines that there are group members or downstream routers, or until a prune message is received from a downstream router. Then, the dense mode interface periodically forwards multicast packets out the interface until the same conditions occur. Dense mode assumes that multicast group members are present. Dense mode routers never send a join message. They do send prune messages as soon as they determine they have no members or downstream PIM routers. A dense mode interface is subject to multicast flooding by default.

Dense Mode with Proxy Registering

For a router in a PIM sparse mode (PIM-SM) domain configured to operate in sparse mode or sparse-dense mode, the **ip pim dense-mode proxy-register** command must be configured on the interface leading toward the bordering dense mode region. This configuration will enable the router to register traffic from the dense mode region with the rendezvous point (RP) in the sparse mode domain.

Prior to Cisco IOS Release 12.0S, an RP needed to be running on the border router leading toward a dense mode region so that the RP could learn about traffic from sources in the dense mode region.

This command requires an extended access list or route map argument specifying which traffic the router needs to register with the RP. This command applies only to sources reachable through a PIM router. Cisco IOS software will always register traffic from remote sources if it arrives on a dense mode interface and if the Reverse Path Forwarding (RPF) neighbor leading toward the source is a Distance Vector Multicast Routing Protocol (DVMRP) but not a PIM router. This functionality has existed since Cisco IOS Release 10.0 and cannot be modified (restricted) with an access list or route map.

Passive Mode

An interface configured with passive mode does not pass or forward PIM control plane traffic; it passes or forwards only IGMP traffic. If passive mode is configured on an interface enabled for IP multicast, the router will not send PIM messages on the interface nor will it accept PIM messages from other routers on this interface. The router acts as the only PIM router on the network and works as the designated router (DR) and the designated forwarder (DF) for all Bidirectional PIM group ranges.

The **ip pim neighbor-filter** command has no effect and is superseded by the **ip pim passive** command when both commands are configured on the same interface.

Do not use the **ip pim passive** command on LANs that have more than one IP multicast router connected to them, because all routers with this command become DR and DF, resulting in duplicate traffic (PIM-SM, PIM-DM, PIM-SSM) or looping traffic (Bidir-PIM). To limit PIM messages to and from valid routers on LANs with more than one router, use the **ip pim neighbor-filter** command

Sparse Mode

A sparse mode interface is used for multicast forwarding only if a join message is received from a downstream router or if group members are directly connected to the interface. Sparse mode assumes that no other multicast group members are present. When sparse mode routers want to join the shared path, they periodically send join messages toward the RP. When sparse mode routers want to join the source path, they periodically send join messages toward the source; they also send periodic prune messages toward the RP to prune the shared path.

Sparse-Dense Mode

An alternative to choosing just dense mode or just sparse mode is to run PIM in a single region in sparse mode for some groups and dense mode for other groups.

In sparse-dense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is “sparse” if the router knows about an RP for that group.

When an interface is treated in dense mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- Any of the PIM neighbors on the interface have not pruned for the group.

When an interface is treated in sparse mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- A PIM neighbor on the interface has received an explicit join message.

Examples

The following example shows how to enable PIM-SM on tunnel interface 0 and set the address of the RP router to 226.0.0.8:

```
ip pim rp-address 226.0.0.8
interface tunnel 0
 ip pim sparse-mode
```

The following example shows how to enable PIM dense mode (PIM-DM) on Ethernet interface 1:

```
interface ethernet 1
 ip pim dense-mode
```

The following example shows how to enable PIM sparse-dense mode on Ethernet interface 1:

```
interface ethernet 1
 ip pim sparse-dense-mode
```

The following example shows how to register the multicast traffic for any source and any multicast group:

```
interface ethernet 0
 ip address 172.16.0.0 255.255.255.0
 description Ethernet interface toward the PIM sparse-mode domain
 ip pim sparse-dense-mode
!
interface ethernet 1
 ip address 172.44.81.5 255.255.255.0
 description Ethernet interface toward the PIM dense-mode region
 ip pim dense-mode proxy-register list 100
!
access-list 100 permit ip any any
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip pim neighbor-filter	Filters PIM messages.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
show ip pim interface	Displays information about interfaces configured for PIM.

ip pim autorp listener

To cause IP multicast traffic for the two Auto-RP groups 224.0.1.39 and 224.0.1.40 to be Protocol Independent Multicast (PIM) dense mode flooded across interfaces operating in PIM sparse mode, use the ip pim autorp listener command in global configuration mode. To disable this feature, use the **no** form of this command.

ip pim autorp listener

no ip pim autorp listener

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip pim autorp listener** command with interfaces configured for PIM sparse mode operation in order to establish a network configuration where Auto-RP operates in PIM dense mode and multicast traffic can operate in sparse mode, bidirectional mode, or Source Specific Multicast (SSM) mode.

Examples

The following example enables IP multicast routing and the Auto-RP listener feature on a router. It also configures the router as a candidate RP for the multicast groups 239.254.2.0 through 239.254.2.255.

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
access-list 1 permit 239.254.2.0 0.0.0.255
```

ip pim dm-fallback

To enable Protocol Independent Multicast (PIM) dense mode (DM) fallback, use the **ip pim dm-fallback** command in global configuration mode. To prevent PIM dense mode fallback, use the **no** form of this command.

ip pim dm-fallback

no ip pim dm-fallback

Syntax Description

This command has no arguments or keywords.

Command Default

PIM dense mode fallback is enabled for all interfaces on the router that are configured with either the **ip pim dense-mode**or **ip pim sparse-dense-mode** commands.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If you use IP multicast in mission-critical networks, you should avoid the use of PIM-DM (dense mode).

Dense mode fallback describes the event of the PIM mode changing (falling back) from sparse mode (which requires an RP) to dense mode (which does not use an RP). Dense mode fallback occurs when RP information is lost.

If all interfaces are configured with the **ip pim sparse-mode** command, there is no dense mode fallback because dense mode groups cannot be created over interfaces configured for sparse mode.

Use the **no ip pim dm-fallback** command to disable PIM-DM flooding on sparse-dense interfaces.

Cause and Effect of Dense Mode Fallback

PIM determines whether a multicast group operates in PIM-DM or PIM-SM mode based solely on the existence of RP information in the group-to-RP mapping cache. If Auto-RP is configured or a bootstrap router (BSR) is used to distribute RP information, there is a risk that RP information can be lost if all RPs, Auto-RP, or the

BSR for a group fails due to network congestion. This failure can lead to the network either partially or fully falling back into PIM-DM.

If a network falls back into PIM-DM and AutoRP or BSR is being used, dense mode flooding will occur. Routers that lose RP information will fallback into dense mode and any new states that must be created for the failed group will be created in dense mode.

Effects of Preventing Dense Mode Fallback

Prior to the introduction of PIM-DM fallback prevention, all multicast groups without a group-to-RP mapping would be treated as dense mode.

With the introduction of PIM-DM fallback prevention, the PIM-DM fallback behavior has been changed to prevent dense mode flooding. By default, if all of the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command), there is no need to configure the **no ip pim dm-fallback** command (that is, the PIM-DM fallback behavior is enabled by default). If any interfaces are not configured using the **ip pim sparse-mode**command (for example, using the **ip pim sparse-dense-mode** command), then the PIM-DM fallback behavior can be explicit disabled using the **no ip pim dm-fallback**command.

When the **no ip pim dm-fallback** command is configured or when **ip pim sparse-mode** is configured on all interfaces, any existing groups running in sparse mode will continue to operate in sparse mode but will use an RP address set to 0.0.0.0. Multicast entries with an RP address set to 0.0.0.0 will exhibit the following behavior:

- Existing (S, G) states will be maintained.
- No PIM Join or Prune messages for (*, G) or (S, G, RPbit) are sent.
- Received (*, G) or (S, G, RPbit) Joins or Prune messages are ignored.
- No registers are sent and traffic at the first hop is dropped.
- Received registers are answered with register stop.
- Asserts are unchanged.
- The (*, G) outgoing interface list (olist) is maintained only for the Internet Group Management Protocol (IGMP) state.
- Multicast Source Discovery Protocol (MSDP) source active (SA) messages for RP 0.0.0.0 groups are still accepted and forwarded.

Examples

The following example shows how to disable PIM-DM fallback:

```
no ip pim dm-fallback
```

Related Commands

Command	Description
ip pim dense-mode	Enables PIM dense mode on the interface.
ip pim sparse-dense-mode	Enables PIM to operate in sparse or dense mode, depending on the group.

ip pim query-interval

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

ip pim query-interval *period* **[msec]**

no ip pim query-interval

Syntax Description

period	The number of seconds or milliseconds (ms) that can be configured for the PIM hello (query) interval. The range is from 1 to 65535.
msec	(Optional) Specifies that the interval configured for the *period* argument be interpreted in milliseconds. If the **msec** keyword is not used along with the *period* argument, the interval range is assumed to be in seconds.

Command Default

PIM hello (query) messages are sent every 30 seconds.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	The **msec** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use this command to configure the frequency of PIM neighbor discovery messages. By default these messages are sent once every 30 seconds. In PIM Version 1 (PIMv1), these messages are referred to as PIM query messages; in PIM Version 2 (PIMv2), these messages are referred to as PIM hello messages. By default, routers run PIMv2 and send PIM hello messages. A router will change (auto-fallback) to PIMv1 and will send PIM query messages if it detects a neighboring router that only supports PIMv1. As soon as that neighboring PIMv1 router is removed from the network, the router will revert to PIMv2.

Note A router can be configured to exclusively use PIMv1 on an interface with the **ip pim version 1** command.

Note In PIM version 2, PIM hello messages also contain a variety of options that allow PIM routers on the network to learn about the capabilities of PIM neighbors. For more information about these capabilities, see the **show ip pim neighbor** command page.

PIM neighbor discovery messages are used to determine which router on a network is acting as the Designated Router (DR) for PIM sparse mode (PIM-SM) and Source Specific Multicast (SSM). The DR is responsible for joining PIM-SM and SSM groups receiving multicast traffic from sources requested by receivers (hosts). In addition, in PIM-SM, the DR is also responsible for registering local sources with the RP. If the DR fails, a backup router will become the DR and then forward traffic for local receivers and register local sources.

The *period* argument is used to specify the PIM hello (query) interval. The interval determines the frequency at which PIM hello (query) messages are sent.

Note When an interfaces enabled for PIM comes up, a PIM hello (query) message is sent immediately. In some cases, the initial PIM hello (query) message may be lost.If the first PIM hello (query) does not get sent when an interface initially comes up, another one will be sent 3 seconds later regardless of the PIM hello (query) interval to ensure that there are no initialization delays.

The configured PIM hello interval also determines the holdtime used by a PIM router. The Cisco IOS software calculates the holdtime as follows:

3 * the interval specified for the *period* argument

By default, PIM routers announce the holdtime in PIM hello (query) messages.If the holdtime expires and another router has not received another hello (query) message from this router, it will timeout the PIM neighbor. If the timed out router was the DR, the timeout will trigger DR election. By default, the DR-failover interval occurs after 90 seconds (after the default holdtime expires for a DR). To reduce DR-failover time in redundant networks, a lower value for the *period* argument can be configured on all routers. The minimum DR-failover time that can be configured (in seconds) is 3 seconds (when the *period* argument is set to 1 second). The DR-failover time can be reduced to less than 3 seconds if the **msecs** keyword is specified. When the **msecs** keyword is used with the **ip pim query-interval** command, the value specified for the *period* argument is interpreted as a value in milliseconds (instead of seconds). By enabling a router to send PIM hello messages more often, this functionality allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently

Note If IGMP Version 1 is being used on a network, then the DR is also the IGMP querier; if at least IGMP version 2 is being used, then the router with the lowest IP address becomes the IGMP querier.

Examples

The following example shows how to set the PIM hello interval to 45 seconds:

```
interface FastEthernet0/1
 ip pim query-interval 45
```

The following example shows how to set the PIM hello interval to 100 milliseconds:

```
interface FastEthernet0/1
 ip pim query-interval 100 msec
```

Related Commands

Command	Description
show ip pim neighbor	Displays information about PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages

ip pim register-rate-limit

To rate limit Protocol Independent Multicast sparse mode (PIM-SM) register packets based on either packets per second or bits per second, use the **ip pim register-rate-limit** command in global configuration mode. To disable this limit, use the **no** form of this command.

Cisco IOS Releases Prior to Releases 12.2(33)SRE and 15.0(1)M

ip pim [**vrf** *vrf-name*] **register-rate-limit** *packets-per-second*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Cisco IOS Releases 12.2(33)SRE, 15.0(1)M, and Cisco IOS XE Release 2.1, and Subsequent 12.2SR, 15.0 Mainline, T Releases, and Cisco IOS XE Releases

ip pim [**vrf** *vrf-name*] **register-rate-limit** *bits-per-second*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Syntax Description

vrf *vrf-name*	(Optional) Rate limits PIM-SM register packets associated with the Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name*argument.
packets-per-second	Maximum number of register packets sent per second by the router. The range is from 1 to 65535 seconds. By default, a maximum rate is not set.
bits-per-second	Maximum number of register bits sent per second. The range is from 8000 to 2000000000 bits. By default, a maximum rate is not set.

Command Default

No rate limit is set for PIM-SM register packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of a bits per second on a per-RP basis.
15.0(1)M	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of bits per second on a per-RP basis.
12.2(33)SRE	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of bits per second on a per-RP basis.

Usage Guidelines

Use this command to rate limit the PIM-SM register packets based on either packets per second or bits per second. Enabling this command will limit the load on the DR and RP at the expense of dropping those register packets that exceed the set limit. Receivers may experience data packet loss within the first second in which register packets are sent from bursty sources.

Setting a value for the *packets-per-second* argument using the **ip pim register-rate-limit**command sets rate limiting on all PIM-SM registers.

Setting a value for the *bits-per-second* argument using the **ip pim register-rate-limit**command sets rate limiting on PIM-SM registers on a per-RP basis.

If the **ip pim**command is configured with the **dense-mode**and **proxy-register**keywords, you must set a limit on the maximum number of PIM-SM register packets sent because of the potentially large number of sources from the dense mode area that may send data into the sparse mode region (and thus need registering in the border router).

This command applies only to sparse mode (S, G) multicast routing entries.

Examples

The following example shows how to configure the **ip pim register-rate-limit**command with a maximum rate of two register packets per second:

```
ip pim register-rate-limit 2
```

The following examples shows how to configure the **ip pim register-rate-limit** command with a maximum rate of 8000 bits per second:

```
ip pim register-rate-limit 8000
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim rp-announce-filter

To filter incoming rendezvous point (RP) announcement messages sent from candidate RPs (C-RPs) to the RP mapping agent, use the **ip pim rp-announce-filter** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-announce-filter** {**group-list** *access-list*| **rp-list** *access-list* [**group-list** *access-list*]}

no ip pim [**vrf** *vrf-name*] **rp-announce-filter** {**group-list** *access-list*| **rp-list** *access-list* [**group-list** *access-list*]}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the filter be applied to incoming RP messages sent from C-RPs associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-list *access-list*	Specifies the number or name of a standard access list that defines the multicast groups to be permitted or denied from RP announcements sent by C-RPs to the RP mapping agent.
rp-list *access-list*	Specifies the number or name of a standard access list that defines the IP addresses of C-RPs whose RP announcements are to be permitted or denied by the RP mapping agent.

Command Default

All RP announcements are accepted by the RP mapping agent.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip pim rp-announce-filter** command to filter incoming Auto-RP announcement messages sent from C-RPs to RP mapping agents. This command should only be configured on RP mapping agents.

Auto-RP provides a means to distribute group-to-RP mappings within a multicast network without having to manually configure static RPs on every router. To accomplish this distribution, Auto-RP uses the following mechanisms:

- C-RPs send RP announcements to multicast group 224.0.1.39.
- RP mapping agents receive the RP announcements from C-RPs and determine which C-RP should be the RP for any given group (or groups) based on the highest IP address. RP mapping agents then distribute that information to all multicast routers by means of RP discovery messages, which are sent to the Auto-RP multicast group address 224.0.1.40.
- The sending of both RP announcements and RP discovery messages occurs every 60 seconds by default with a holdtime of 180 seconds. If no RP is found, each router then searches locally for a static RP mapping. If no static RP mapping is configured, the router defaults to dense mode.

The **ip pim rp-announce filter** command allows you to configure policies on an RP mapping agent that define the C-RPs whose RP announcements are to be filtered (ignored) by the mapping agent. You can use this command to configure the mapping agent to filter RP announcement messages from specific or unknown routers by permitting or denying specific C-RPs .You can also filter RP announcement messages from an candidate RP for specific group prefixes, thereby restricting that router to be the C-RP for only the ranges not filtered on the RP mapping agent.

Caution If you use more than one RP-mapping agent, you must configure the same filters on all mapping agents to avoid inconsistencies in Auto-RP operations.

Caution An improperly configured **ip pim rp-announce-filter**command may result in RP announcements being ignored. In addition, the **ip pim rp-announce-filter** command should only be configured on the mapping agent; if not, the command will fail because non-mapping agents do not listen to group 224.0.1.39 and do not know how to distribute the necessary group-to-RP mappings.

Use the **rp-list** keyword and *access-list* argument to specify the standard access list that defines the IP addresses of C-RPs whose RP announcements are to be permitted or denied on the RP mapping agent. Use the **group-list**keyword and *access-list* argument to specify the standard access list that defines the multicast groups to be permitted or denied from RP announcements sent by C-RPs to the RP mapping agent. RP announcment messages received that match the access list specified for **rp-list** keyword and access list specified for the **group-list** keyword are filtered by the RP mapping agent.

If a C-RP list is not specified (using the **rp-list** keyword and *access-list*argument), the command will permit all C-RPs. If a group list is not specified (using the **group-list** keyword and *access-list* argument), the command will deny all groups.

If no **ip pim rp-announce-filter** commands are configured, a router enabled to be an RP mapping agent (using the **ip pim send-rp-discovery** command) will accept all RP announcements for all groups from all C-RPs. Configure one or more **ip pim rp-announce-filter**commands on RP mapping agents to filter unwanted RP messages.

Examples

The following example shows how to configure the router to accept RP announcements from the C-RPs defined in access list 1 for the group range defined in access list 2:

```
ip pim rp-announce-filter rp-list 1 group-list 2
access-list 1 permit 10.0.0.1
access-list 1 permit 10.0.0.2
access-list 2 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim send-rp-discovery	Configures the router to be an RP mapping agent.

ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this router as an RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** {*interface-type interface-number*| *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] **[bidir]**

no ip pim [**vrf** *vrf-name*] **send-rp-announce** {*interface-type interface-number*| *ip-address*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and number that is used to define the RP address. No space is required between the values.
ip-address	IP address of the RP for the group. The IP address must be a directly connected address. If the command is configured with this argument, the RP-announce message will be sourced by the interface to which this IP address is connected (that is, the source address in the IP header of the RP-announce message is the IP address of that interface).
scope *ttl-value*	Specifies the time-to-live (TTL) value that limits the number of Auto-RP announcements.
group-list *access-list*	(Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Specifies the interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds.

bidir	(Optional) Indicates that the multicast groups specified by the *access-list*argument are to operate in bidirectional mode. If the command is configured without this keyword, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).

Command Default Auto-RP is disabled.*seconds*: 60

Command Modes Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(2)T	This command was modified. The following keywords and argument were added: • **interval** *seconds* • **bidir**
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(5)	This command was modified. The *ip-address* argument was added.
12.3(17)	This command was modified. The *ip-address* argument was added.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The *ip-address* argument was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE release 3.3SG	This command was integrated into Cisco IOS XE release 3.3SG.

Usage Guidelines

Enter this command on the router that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send 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 RP for the groups in the range described by the access list.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-RP mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address**command.

Examples

The following example shows how to configure the router to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as RP is the IP address associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as RP.

```
ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.

ip pim send-rp-discovery

To configure the router to be a rendezvous point (RP) mapping agent, use the **ip pim send-rp-discovery**command in global configuration mode. To deconfigure the router from functioning as the RP mapping agent, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]

no ip pim [**vrf** *vrf-name*] **send-rp-discovery**

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to be an RP mapping agent for the specified Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance.
interface-type interface-number	(Optional) Interface type and number that is to be used as the source address of the RP mapping agent.
scope *ttl-value*	Specifies the time-to-live (TTL) value for Auto-RP discovery messages. The range is from 1 to 255.
interval *seconds*	(Optional) Specifies the interval at which Auto-RP discovery messages are sent. The range is from 1 to 16383. **Note** By default, Auto-RP discovery messages are sent at an interval of 60 seconds or when the RP mapping agent detects changes.

Command Default

The router is not configured to be an RP mapping agent.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(8)	The **interval** keyword and *seconds* argument were added.
12.4(9)T	The **interval** keyword and *seconds* argument were added.
12.2(33)SRB	The **interval** keyword and *seconds* argument were added.
12.2(18)SXF11	The **interval** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip pim send-rp-discovery** command to configure the router to be an RP mapping agent. An RP mapping agent receives Auto-RP announcement messages, which it stores in its local group-to-RP mapping cache. The RP mapping agent uses the information contained in the Auto-RP announcement messages to elect the RP. The RP mapping agent elects the candidate RP with the highest IP address as the RP for a group range.

The required **scope** keyword and *ttl-value* argument are used to specify the TTL value in the IP header of Auto-RP discovery messages.

Note For the **scope** keyword and *ttl-value* argument, specify a TTL large enough to cover your Protocol Independent Multicast (PIM) domain.

The optional **interval** keyword and *seconds* argument are used to specify the interval at which Auto-RP discovery messages are sent. By default, Auto-RP discovery messages are sent at an interval of 60 seconds or when the RP mapping agent detects changes.

Note Lowering the interval at which Auto-RP discovery messages are sent from the default value of 60 seconds results in more frequent floodings of the group-to-RP mappings. In some network environments, the disadvantages of lowering the interval (more control packet overhead) may outweigh the advantages (more frequent group-to-RP mapping updates).

When Auto-RP is used, the following events occur:

1. The RP mapping agent listens for Auto-RP announcement messages sent by candidate RPs to the well-known group address CISCO-RP-ANNOUNCE (224.0.1.39).
2. The RP mapping agents stores the information learned from Auto-RP announcement messages in its local group-to-RP mapping cache.
3. The RP mapping agents elects the candidate RP with the highest IP address as the RP and announces the RP in the Auto-RP discovery messages that it sends out.
4. The Auto-RP discovery messages that the RP mapping agent sends to the well-known group CISCO-RP-DISCOVERY (224.0.1.40), which Cisco routers join by default, contains the elected RP learned from the RP mapping agent's group-to-RP mapping cache.

5 PIM designated routers listen for the Auto-RP discovery messages sent to 224.0.1.40 to learn the RP and store the information about the RP in their local group-to-RP mapping caches.

Use the **show ip pim rp** command with the **mapping** keyword to display all the group-to-RP mappings that the router has learned from Auto-RP.

Examples

The following example shows how to configure a router to be an RP mapping agent. In this example, the RP mapping agent is configured to use loopback 0 as the source address for Auto-RP messages. The Auto-RP discovery messages sent by the RP mapping agent are configured to be sent out at an interval of 50 seconds with a TTL of 20 hops.

```
ip pim send-rp-discovery loopback 0 scope 20 interval 50
```

Related Commands

Command	Description
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.

ip pim spt-threshold

To configure when a Protocol Independent Multicast (PIM) leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold**command in global configuration mode. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps*| **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps*| **infinity**} [**group-list** *access-list*]

Cisco IOS T-Train Release

ip pim [**vrf** *vrf-name*] **spt-threshold** {**0**| **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {**0**| **infinity**} [**group-list** *access-list*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
kbps	Traffic rate; valid values are from 0 to 4294967 kbps.
infinity	Causes all sources for the specified group to use the shared tree.
group-list *access-list*	(Optional) Specifies the groups to which the threshold applies. Must be an IP standard access list number or name. If the value is 0, the threshold applies to all groups.
0	Specifies to always switch to the source tree.

Command Default

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If a source sends at a rate greater than or equal to traffic rate (the *kbps* value), a PIM join message is triggered toward the source to construct a source tree.

If the **infinity** keyword is specified, all sources for the specified group will use the shared tree. Specifying a **group-list** *access-list* indicates the groups to which the threshold applies.

If the traffic rate from the source drops below the threshold traffic rate, the leaf router will switch back to the shared tree and send a prune message toward the source.

Examples

The following example shows how to set a threshold of 4 kbps. If the traffic rate exceeds this threshold, the traffic to a group from a source causes the router to switch to the shortest path tree to that source.

```
Router# configure terminal
Router(config)# ip pim spt-threshold 4
```

Related Commands

Command	Description
ip pim bidir-neighbor-filter	Configures an ACL to specify which bidirectionally capable neighbors will participate in the designated forwarder election.

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **ssm** {**default**| **range** *access-list*}

no ip pim [**vrf** *vrf-name*] **ssm** {**default**| **range** *access-list*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
default	Defines the SSM range access list to 232/8.
range *access-list*	Specifies the standard IP access list number or name defining the SSM range.

Command Default

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

Examples

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

```
access-list 4 permit 224.2.151.141
ip pim ssm range 4
```

Related Commands

Command	Description
ip igmp v3lite	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
ip urd	Enables interception of TCP packets sent to the reserved URD port 659 on an interface and processing of URD channel subscription reports.

ip pim state-refresh disable

To disable the processing and forwarding of PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh disable**command in global configuration mode. To reenable the processing and forwarding of PIM dense mode state refresh control messages, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **state-refresh disable**

no ip pim [**vrf** *vrf-name*] **state-refresh disable**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Default

The processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports the PIM dense mode state refresh feature.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Configuring this command removes PIM dense mode state refresh information from PIM hello messages.

Examples

The following example shows how to disable the periodic forwarding of the PIM dense mode state refresh control message down a source-based IP multicast distribution tree:

```
ip pim state-refresh disable
```

Related Commands

Command	Description
ip pim state-refresh origination-interval	Configures the origination of and the interval for the PIM dense mode state refresh control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

ip pim state-refresh origination-interval

To configure the origination of and the interval for PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh origination-interval**command in interface configuration mode. To stop the origination of the PIM dense mode state refresh control message, use the **no** form of this command.

ip pim state-refresh origination-interval [*interval*]

no ip pim state-refresh origination-interval [*interval*]

Syntax Description

interval	(Optional) The number of seconds between PIM dense mode state refresh control messages. The default is 60 seconds. The available interval range is from 4 to 100 seconds.

Command Default

PIM dense mode state refresh control message origination is disabled. By default, all PIM routers that are running a Cisco IOS software release that supports PIM dense mode state refresh can process and forward PIM dense mode state refresh control messages.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)S	This command was modified. This command can be now be configured on an interface that is not enabled for PIM dense mode.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Configure this command on the interfaces of the first hop, PIM dense mode routers that are directly connected to sources for PIM-DM multicast groups.

In Cisco IOS Release 15.1(1)S and later releases, this command can be configured on an interface on which PIM sparse mode is enabled.

In Cisco IOS Release 15.1(0)S and earlier releases, this command can be configured on an interface only if PIM dense mode state refresh is enabled. If you attempt to configure this command on an interface on which PIM sparse mode is enabled, the following warning message is displayed.

```
Warning: PIM State-Refresh cannot be configured on sparse interface
```

By default, the processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports PIM dense mode state refresh.

Examples

The following example configures the origination of the state refresh control message on Ethernet interface 0 of a PIM dense mode router with an interval of 80 seconds:

```
interface ethernet 0
 ip pim state-refresh origination-interval 80
```

Related Commands

Command	Description
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh feature control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

ip rgmp

To enable the Router-Port Group Management Protocol (RGMP) on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, use the **ip rgmp**command in interface configuration mode. To disable RGMP on the interfaces, use the **no** form of this command.

ip rgmp

no ip rgmp

Syntax Description

This command has no arguments or keywords.

Command Default

RGMP is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)S	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

RGMP is supported only on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.

Before you enable RGMP, the following features must be enabled on your router:

- IP routing
- IP multicast
- PIM in sparse mode, sparse-dense mode, source specific mode, or bidirectional mode

If your router is in a bidirectional group, make sure to enable RGMP only on interfaces that do not function as a designated forwarder (DF). If you enable RGMP on an interface that functions as a DF, the interface will not forward multicast packets up the bidirectional shared tree to the rendezvous point (RP).

The following features must be enabled on your switch:

- IP multicast

- IGMP snooping

Examples

The following example enables RGMP on Ethernet interface 1/0:

```
interface ethernet 1/0
 ip rgmp
```

Related Commands

Command	Description
debug ip rgmp	Logs debug messages sent by an RGMP-enabled router.
show ip igmp interface	Displays multicast-related information about an interface.

manager

To specify the interface that is to act as the Manager for Multicast Routing Monitor (MRM), and to specify the multicast group address the Test Receiver will listen to, use the **manager**command in MRM manager configuration mode. To remove the Manager or group address, use the **no** form of this command.

manager *interface-type interface-number* **group** *ip-address*

no manager *interface-type interface-number* **group** *ip-address*

Syntax Description

interface-type interface-number	Interface type and number of the Manager. The IP address associated with this interface is the source address of the Manager.
group *ip-address*	Specifies the IP multicast group address that the Test Receiver will listen to.

Command Default

There is no MRM Manager configured.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command identifies the interface that acts as the Manager, and therefore is required in order to run MRM.

Examples

The following example shows how to configure Ethernet interface 0 as the Manager and the Test Receiver to listen to multicast group 239.1.1.1:

```
ip mrm manager test1
 manager ethernet 0 group 239.1.1.1
```

Related Commands

Command	Description
beacon (multicast routing monitor)	Changes the frequency, duration, or scope of beacon messages that the Manager sends to Test Senders and Test Receivers during an MRM test.
ip mrm accept-manager	Configures a Test Sender or Test Receiver to accept requests only from Managers that pass an access list.
show ip mrm manager	Displays test information for MRM.

S

show ip igmp groups

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

show ip igmp [**vrf** *vrf-name*] **groups** [*group-name*| *group-address*| *interface-type interface-number*] **[detail]**

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance and indicates the name assigned to the VRF.
group-name	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted-decimal notation.
interface-type interface-number	(Optional) Interface type and Interface number.
detail	(Optional) Provides a detailed description of the sources known through IGMP Version 3 (IGMPv3), IGMPv3lite, or URL Rendezvous Directory (URD).

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	Fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.
12.1(5)T	The **detail**keyword was added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	A field was added to the output of this command to support the SSM mapping feature.

Release	Modification
12.2(18)S	A field was added to the output of this command to support the SSM mapping feature.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip igmp groups** command displays by group address, interface type, and interface number all directly connected multicast groups.

Examples

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

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address     Interface         Uptime      Expires     Last Reporter
239.255.255.254   Ethernet3/1       1w0d        00:02:19    172.21.200.159
224.0.1.40        Ethernet3/1       1w0d        00:02:15    172.21.200.1
224.0.1.40        Ethernet3/3       1w0d        never       172.16.214.251
224.0.1.1         Ethernet3/1       1w0d        00:02:11    172.21.200.11
224.9.9.2         Ethernet3/1       1w0d        00:02:10    172.21.200.155
232.1.1.1         Ethernet3/1       5d21h       stopped     172.21.200.206
```

The following is sample output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword:

```
Router# show ip igmp groups 192.168.1.1 detail
Interface:      Ethernet3/2
Group:          192.168.1.1
Uptime:         01:58:28
Group mode:     INCLUDE
Last reporter:  10.0.119.133
CSR Grp Exp:    00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote
                    S- Static, M - SSM Mapping)
  Source Address   Uptime    v3 Exp    CSR Exp   Fwd  Flags
  172.16.214.1     01:58:28  stopped   00:02:31  Yes  C
```

The table below describes the significant fields shown in the displays.

Table 1: show ip igmp groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.

Field	Description
Uptime	Time in weeks, days, hours, minutes, and seconds that this multicast group has been known.
Expires	Time in weeks, days, hours, minutes, and seconds until the entry expires. If an entry expires, then the entry (for a short period) shows “now” before it is removed. “never” indicates that the entry will not time out, because a local receiver is on this router for this entry. “stopped” indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports that are received on the interface for the group. In the output for the **show ip igmp groups detail** command, the EXCLUDE mode also shows the Expires: field for the group entry (not shown in the output).
CSR Grp Exp	Shown for multicast groups in the SSM range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but they do not indicate group membership by themselves.
Group source list:	Details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Time since the source state was created.
v3 Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP operations. “stopped” displays if no member uses IGMPv3 (but only IGMP v3lite or URD).

Field	Description
CSR Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP v3lite or URD reports. “stopped” displays if members use only IGMPv3.
Fwd	Status of whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
show ip igmp ssm-mapping	Displays information about SSM mapping or displays the sources that SSM mapping uses for a particular group.

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** command in user EXEC or privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **interface** [*interface-type interface-number*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

This command also displays information about dynamically learned Distance Vector Multicast Routing Protocol (DVMRP) routers on the interface.

Examples

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

```
Router# show ip igmp interface
Ethernet0 is up, line protocol is up
  Internet address is 192.168.37.6, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.37.33
  No multicast groups joined
Ethernet1 is up, line protocol is up
  Internet address is 192.168.36.129, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.36.131
  Multicast groups joined: 225.2.2.2 226.2.2.2
Tunnel0 is up, line protocol is up
  Internet address is 10.1.37.2, subnet mask is 255.255.0.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  No multicast groups joined
```

The table below describes the significant fields shown in the display.

Table 2: show ip igmp interface Field Descriptions

Field	Description
Ethernet0 is up, line protocol is up	Interface type, number, and status.
Internet address is..., subnet mask is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the **ip address** command.
IGMP is enabled on interface	Indicates whether IGMP has been enabled on the interface with the **ip pim**command.
IGMP query interval is 60 seconds	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages, as specified with the **ip igmp query-interval** command.
Inbound IGMP access group is not set	Indicates whether an IGMP access group has been configured with the **ip igmp access-group** command.
Multicast routing is enabled on interface	Indicates whether multicast routing has been enabled on the interface with the **ip pim**command.
Multicast TTL threshold is 0	Packet time-to-live threshold, as specified with the **ip multicast ttl-threshold** command.

Field	Description
Multicast designated router (DR) is...	IP address of the designated router for this LAN segment (subnet).
No multicast groups joined	Indicates whether this interface is a member of any multicast groups and, if so, lists the IP addresses of the groups.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.
ip multicast ttl-threshold	Configures the TTL threshold of packets being forwarded out an interface.
ip pim	Enables PIM on an interface.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of a device, use the **show ip igmp snooping**command in user EXEC or privileged EXEC mode.

show ip igmp snooping [**groups** [**count**| **vlan** *vlan-id* [*ip-address*| **count**]]| **mrouter** [[**vlan** *vlan-id*]| [**bd** *bd-id*]] | **querier**| **vlan** *vlan-id*| **bd** *bd-id*]

Syntax Description

groups	(Optional) Displays group information.
count	(Optional) Displays the number of multicast groups learned by IGMP snooping.
vlan *vlan-id*	(Optional) Specifies a VLAN. Valid values are 1 to 1001. If this keyword is not configured, information is displayed for all VLANs.
bd *bd-id*	(Optional) Specifies a bridge domain. Valid values are 1 to 1001. If this keyword is not configured, information is displayed for all bridge domains.
ip-address	(Optional) Displays information about the specified group.
count	(Optional) Displays group count inside a VLAN.
mrouter	(Optional) Displays information about dynamically learned and manually configured multicast router ports.
querier	(Optional) Displays IGMP querier information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Release	Modification
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC on Cisco 870 series Integrated Services Routers (ISRs). The **groups** and **querier** keywords were added.
12.4(15)T	The **groups** and **count** keywords were added on the Cisco 87x and the Cisco 1800 series Integrated Services Routers (ISRs) and on EtherSwitch high-speed WAN interface cards (HWICs) and EtherSwitch network modules running on the Cisco 1841, 2800, and 3800 series ISRs.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. The **bd** *bd-id* keyword and argument combination was added.

Usage Guidelines

You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

Examples

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

```
Router# show ip igmp snooping

Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last Member Query Interval : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Enabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
Last Member Query Interval           : 1000
CGMP interoperability mode           : IGMP_ONLY

Vlan 11:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
Last Member Query Interval           : 1000
CGMP interoperability mode           : IGMP_ONLY
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping**command using the **vlan** keyword:

```
Router# show ip igmp snooping vlan 1vlan 1
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping**command using the **bd** keyword:

```
show ip igmp snooping bd 101
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State     : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
EHT DB limit/count           : 100000/0
TCN solicit query            : Disabled
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No
.
.
.
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping**command using the **mrouter** keyword:

Note In this example, Fa0/3 is a dynamically learned router port, and Fa0/2 is a configured static router port.

```
Router# show ip igmp snooping mrouter vlan 1
Vlan    ports
----    -----
   1    Fa0/2(static), Fa0/3(dynamic)
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping** command using the **groups**keyword:

```
Router #show ip igmp snooping groups
Vlan      Group          Version     Port List
------------------------------------------------------------
1         192.168.1.2      v2          Fa0/1/0
11        192.168.1.2      v2          Fa0/1/1
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping groups** command with the **count** keyword specified:

```
Router# show ip igmp snooping groups count

Total number of groups:   2
```

The information in the output is self-explanatory.

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.

Command	Description
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp snooping mrouter

Note The documentation for this command has been integrated into the documentation for the **show ip igmp snooping** command. Please see the **show ip igmp snooping** command for complete and up-to-date information about displaying information for dynamically learned and manually configured multicast router ports.

To display information on dynamically learned and manually configured multicast router ports, use the **show ip igmp snooping mrouter**command in privileged EXEC mode.

show ip igmp snooping mrouter {**vlan** *vlan-id*| **bd** *bd-id*}

Syntax Description

vlan *vlan-id*	Specifies a VLAN. Valid values are 1 to 1001.
bd *bd-id*	Specifies a bridge domain. Valid values are 1 to 16823.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.5S	This command was modified. The **bd** *bd-id* keyword and argument were added.

Usage Guidelines

You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has Internet Group Management Protocol (IGMP) snooping enabled.

Examples

The following is sample output from the **show ip igmp snooping mrouter vlan 1**command:

Note In this example, Fa0/3 is a dynamically learned router port, and Fa0/2 is a configured static router port.

```
Router# show ip igmp snooping mrouter vlan 1Vlan     ports
----     -----
   1     Fa0/2(static), Fa0/3(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp udlr

To display unidirectional link routing (UDLR) information for directly connected multicast groups on interfaces that have a unidirectional link (UDL) helper address configured, use the **show ip igmp udlr**command in user EXEC or privileged EXEC mode.

show ip igmp udlr [*group-name*| *group-address*| *interface-type interface-number*]

Syntax Description

group-name | *group-address*	(Optional) Name or address of the multicast group for which to show UDLR information.
interface-type interface-number	(Optional) Interface type and number for which to show UDLR information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(17d)SXB1	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command displays which groups are being forwarded and received over the UDL.

On the upstream router, this command shows which interface is a UDL interface and which IP multicast groups are being forwarded out that interface. The UDL Reporter is the IP address of the downstream interface on the receiving router. If there is more than one downstream router, this field shows which downstream router forwarded the IGMP host report to the upstream router over the ground-based network. This report is forwarded over the UDL so that all downstream routers know which groups have already been requested by other downstream routers and additional IGMP host reports are suppressed.

On the downstream router, this command (in the Interface field) shows which local interface received an IGMP host report (from a directly connected host for a specific group). The UDL Reporter is the IP address of the router that had forwarded the IGMP host report to the upstream router over the ground-based network. The UDL Interfaces column shows the interface on which IP multicast packets are being received.

Examples

The following is sample output of the **show ip igmp udlr**command on an upstream router:

```
upstream-rtr# show ip igmp udlr
IGMP UDLR Status, UDL Interfaces: Serial0
```

```
Group Address    Interface            UDL Reporter     Reporter Expires
224.2.127.254    Serial0              10.0.0.2         00:02:12
224.0.1.40       Serial0              10.0.0.2         00:02:11
225.7.7.7        Serial0              10.0.0.2         00:02:15
```

The following is sample output of the **show ip igmp udlr**command on a downstream router:

```
downstream-rtr# show ip igmp udlr
IGMP UDLR Status, UDL Interfaces: Serial0
Group Address    Interface            UDL Reporter     Reporter Expires
224.2.127.254    Serial0              10.0.0.2         00:02:49
224.0.1.40       Serial0              10.0.0.2         00:02:48
225.7.7.7        Serial0              10.0.0.2         00:02:52
```

The table below describes the significant fields shown in the first display.

Table 3: show ip igmp udlr Field Descriptions

Field	Description
Group Address	All groups helpered by the UDL Reporter on the interface.
Interface	Interface type and number to which the group is connected.
UDL Reporter	IP address of the router on the UDL network that is IGMP helpering for the group.
Reporter Expires	How soon the UDL Reporter will become inactive, in hours:minutes:seconds. This can occur under the following conditions: • The UDL Reporter has become nonoperational. • The link or network to the reporter has become nonoperational. • The group member attached to the UDL Reporter has left the group.

show ip mroute

To display the contents of the multicast routing (mroute) table, use the **show ip mroute** command in user EXEC or privileged EXEC mode.

show ip mroute [**vrf** *vrf-name*] [[**active** [*kbps*] [**interface** *type number*]| **bidirectional**| **count [terse]**| **dense**| **interface** *type number*| **proxy**| **pruned**| **sparse**| **ssm**| **static**| **summary**]| [*group-address* [*source-address*]] [**count [terse]**| **interface** *type number*| **proxy**| **pruned**| **summary**]| [*source-address group-address*] [**count [terse]**| **interface** *type number*| **proxy**| **pruned**| **summary**]| [*group-address*] **active** [*kbps*] [**interface** *type number*| **verbose**]]

Syntax Description

vrf *vrf-name*	(Optional) Filters the output to display only the contents of the mroute table that pertain to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
active *kbps*	(Optional) Displays the rate that active sources are sending to multicast groups, in kilobits per second (kbps). Active sources are those sending at the *kbps* value or higher. The range is from 1 to 4294967295. The *kbps* default is 4 kbps.
interface *type number*	(Optional) Filters the output to display only mroute table information related to the interface specified for the *type number* arguments.
bidirectional	(Optional) Filters the output to display only information about bidirectional routes in the mroute table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.
terse	(Optional) Filters the output to display a subset of mroute statistics, excluding source and group statistics for each mroute entry in the mroute table.
dense	(Optional) Filters the output to display only information about dense mode routes in the mroute table.
proxy	(Optional) Displays information about Reverse Path Forwarding (RPF) vector proxies received on a multicast router.

pruned	(Optional) Filters the output to display only information about pruned routes in the mroute table.
sparse	(Optional) Filters the output to display only information about sparse mode routes in the mroute table.
ssm	(Optional) Filters the output to display only the Source Specific Multicast (SSM) routes in the mroute table.
static	(Optional) Filters the output to display only the static routes in the mroute table.
summary	(Optional) Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.
group-address	(Optional) IP address or Domain Name System (DNS) name of a multicast group.
source-address	(Optional) IP address or DNS name of a multicast source.
verbose	(Optional) Displays additional information.

Command Default

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the mroute table.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. The H flag for multicast multilayer switching (MMLS) was added in the output display.
12.1(3)T	This command was modified. The U, s, and I flags for SSM were introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.0(30)S	This command was modified. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.

Release	Modification
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S. The **vrf** keyword and *vrf-name* argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.3	This command was modified. The Z, Y, and y flags were introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(6)T	This command was modified. The **terse** keyword was added.
12.4(7)	This command was modified. The **terse** keyword was added.
12.2(18)SXF2	This command was modified. The **terse** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **terse** keyword was added. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
12.2(31)SB2	This command was modified. The E flag for the Multicast VPN Extranet Support feature was introduced. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature. The **terse** keyword was added.
12.2(33)SXH	This command was modified. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
12.2(33)SRC	This command was modified. The E flag for the Multicast VPN Extranet Support feature was introduced.
12.2(33)SRE	This command was modified. The **verbose**keyword was added.
12.4(20)T	This command was modified. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
15.0(1)M	This command was modified. The E flag for the Multicast VPN Extranet Support feature was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.2(3)T	This command was modified. The output was modified to indicate if an outgoing interface is blocked by RSVP multicast CAC.

Release	Modification
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **show ip mroute** command to display information about mroute entries in the mroute table. The Cisco IOS software populates the multicast routing table by creating (S, G) entries from (*, G) entries. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through RPF).

Use the **clear ip mroute** command to delete entries from the mroute table.

Examples

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

The following is sample output from the **show ip mroute** command with the IP multicast group address 232.6.6.6 specified:

```
Router# show ip mroute 232.6.6.6
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 224.0.0.0
  Outgoing interface list:Null

(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags:CTI
  Incoming interface:Ethernet3/3, RPF nbr 224.0.0.0
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 00:00:36/00:02:35
```

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This output displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router# show ip mroute cbone-audio
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 224.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 224.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28
(192.168.37.100, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

The following is sample output from the **show ip mroute** command that shows the virtual circuit descriptor (VCD) value, because an ATM interface with Protocol Independent Multicast (PIM) multipoint signaling is enabled:

```
Router# show ip mroute 224.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 224.1.1.1), 00:03:57/00:02:54, RP 172.16.0.0, flags: SJ
  Incoming interface: Null, RPF nbr 224.0.0.0224.0.0.0
  Outgoing interface list:
    ATM0/0, VCD 14, Forward/Sparse, 00:03:57/00:02:53
```

The following is sample output from the **show ip mroute** command with the **summary** keyword:

```
Router# show ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.255.255.255), 2d16h/00:02:30, RP 172.16.10.13, flags: SJPC
(*, 224.2.127.253), 00:58:18/00:02:00, RP 172.16.10.13, flags: SJC
(*, 224.1.127.255), 00:58:21/00:02:03, RP 172.16.10.13, flags: SJC
(*, 224.2.127.254), 2d16h/00:00:00, RP 172.16.10.13, flags: SJCL
  (172.16.160.67, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
  (172.16.244.217, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
  (172.16.8.33, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
  (172.16.2.62, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
  (172.16.8.3, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
  (172.16.60.189, 224.2.127.254), 00:03:47/00:00:46, flags: CLJT
```

The following is sample output from the **show ip mroute** command with the **active** keyword:

```
Router# show ip mroute active 4
Active IP Multicast Sources - sending >= 4 kbps
Group: 224.2.127.254, (sdr.cisco.com)
```

```
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)
Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

The following partial sample output shows that outbound interface Ethernet 0/2 is blocked. The data flow on an interface can be blocked because RSVP deleted (denial) the reservation for the flow or the flow matched an ACL that is subject to RSVP multicast CAC:

```
mcast-iou01-2# sho ip mro 237.1.1.2
IP Multicast Routing Table
.
.
.
(40.0.7.200, 237.1.1.2), 00:04:34/00:03:15, flags: T
  Incoming interface: Ethernet0/0, RPF nbr 40.0.1.1
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse-Dense, 00:04:34/00:02:57
    Ethernet0/2, Forward/Sparse-Dense, 00:04:16/00:02:33 Blocked
```

The table below describes the significant fields shown in the displays.

Table 4: show ip mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry. • D--Dense. Entry is operating in dense mode. • S--Sparse. Entry is operating in sparse mode. • B--Bidir Group. Indicates that a multicast group is operating in bidirectional mode. • s--SSM Group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes. • C--Connected. A member of the multicast group is present on the directly connected interface.

Field	Description
Flags: (continued)	

Field	Description
	• L--Local. The router itself is a member of the multicast group. Groups are joined locally by the **ip igmp join-group** command (for the configured group), the **ip sap listen** command (for the well-known session directory groups), and rendezvous point (RP) mapping (for the well-known groups 224.0.1.39 and 224.0.1.40). Locally joined groups are not fast switched. • P--Pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source. • R--RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source. • F--Register flag. Indicates that the software is registering for a multicast source. • T--SPT-bit set. Indicates that packets have been received on the shortest path source tree. • J--Join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute. **Note** The router measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval

Field	Description
	is started. If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest path source tree when traffic from a new source is received.

Field	Description
	• M--MSDP created entry. Indicates that a (*, G) entry was learned through a Multicast Source Discovery Protocol (MSDP) peer. This flag is applicable only for an RP running MSDP. • E--Extranet source mroute entry. Indicates that a (*, G) or (S, G) entry in the VRF routing table is a source Multicast VRF (MVRF) entry and has extranet receiver MVRF entries linked to it. • X--Proxy Join Timer Running. Indicates that the proxy join timer is running. This flag is set only for (S, G) entries of an RP or "turnaround" router. A "turnaround" router is located at the intersection of a shared path (*, G) tree and the shortest path from the source to the RP. • A--Candidate for MSDP Advertisement. Indicates that an (S, G) entry was advertised through an MSDP peer. This flag is applicable only for an RP running MSDP. • U--URD. Indicates that a URL Rendezvous Directory (URD) channel subscription report was received for the (S, G) entry. • I--Received Source Specific Host Report. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by Internet Group Management Protocol Version 3 (IGMPv3), URD, or IGMP v3lite. This flag is set only on the designated router (DR). • Z--Multicast Tunnel. Indicates that this entry is an IP multicast group that belongs to the Multicast Distribution Tree (MDT) tunnel. All packets received for this IP multicast state are sent to the MDT tunnel for decapsulation. • Y--Joined MDT-data group. Indicates that the traffic was received through an MDT tunnel that was set up specifically for this source and group. This flag is set in Virtual Private Network (VPN) mroute tables only. • y--Sending to MDT-data group. Indicates that the traffic was sent through an MDT tunnel that was set up specifically for this source and group. This flag is set in VPN mroute tables only.

Field	Description
Outgoing interface flags:	Provides information about the entry. • H--Hardware switched. Indicates that a multicast Multilayer Switching (MMLS) forwarding path has been established for this entry.
Timers:Uptime/Expires	"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
Interface state:	Indicates the state of the incoming or outgoing interface. • Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list. • Next-Hop or VCD. "Next-hop" specifies the IP address of the downstream neighbor. "VCD" specifies the virtual circuit descriptor number. "VCD0" means the group is using the static map virtual circuit. • State/Mode. "State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold. "Mode" indicates whether the interface is operating in dense, sparse, or sparse-dense mode.
(*, 224.0.255.1) and (192.168.37.100, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries. (*, G) entries are used to build (S, G) entries.
RP	Address of the RP router. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
flags:	Information about the entry.

Field	Description
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor or RPF nbr	IP address of the upstream router to the source. Tunneling indicates that this router is sending data to the RP encapsulated in register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used. If an asterisk (*) appears after the IP address in this field, the RPF neighbor has been learned through an assert.
Outgoing interface list:	Interfaces through which packets will be forwarded. When the **ip pim nbma-mode** command is enabled on the interface, the IP address of the Protocol Independent Multicast (PIM) neighbor is also displayed. The Blocked keyword will be displayed in the output if the interface is blocked (denied) by RSVP mulicast CAC.

The following is sample output from the **show ip mroute** command with the **count** keyword:

```
Router# show ip mroute count
IP Multicast Statistics
4045 routes using 2280688 bytes of memory
41 groups, 97.65 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group:239.0.18.1, Source count:200, Packets forwarded:348232, Packets received:348551
  RP-tree:Forwarding:12/0/218/0, Other:12/0/0
  Source:10.1.1.1/32, Forwarding:1763/1/776/9, Other:1764/0/1
  Source:10.1.1.2/32, Forwarding:1763/1/777/9, Other:1764/0/1
  Source:10.1.1.3/32, Forwarding:1763/1/783/10, Other:1764/0/1
  Source:10.1.1.4/32, Forwarding:1762/1/789/10, Other:1763/0/1
  Source:10.1.1.5/32, Forwarding:1762/1/768/10, Other:1763/0/1
  Source:10.1.1.6/32, Forwarding:1793/1/778/10, Other:1794/0/1
  Source:10.1.1.7/32, Forwarding:1793/1/763/10, Other:1794/0/1
  Source:10.1.1.8/32, Forwarding:1793/1/785/10, Other:1794/0/1
  Source:10.1.1.9/32, Forwarding:1793/1/764/9, Other:1794/0/1
  Source:10.1.1.10/32, Forwarding:1791/1/774/10, Other:1792/0/1
  Source:10.1.2.1/32, Forwarding:1689/1/780/10, Other:1691/0/2
  Source:10.1.2.2/32, Forwarding:1689/1/782/10, Other:1691/0/2
  Source:10.1.2.3/32, Forwarding:1689/1/776/9, Other:1691/0/2
.
.
.

Group:239.0.18.132, Source count:0, Packets forwarded:8810, Packets received:8810
  RP-tree:Forwarding:8810/7/780/49, Other:8810/0/0
Group:239.0.17.132, Source count:0, Packets forwarded:704491, Packets received:704491
  RP-tree:Forwarding:704491/639/782/4009, Other:704491/0/0
Group:239.0.17.133, Source count:0, Packets forwarded:704441, Packets received:704441
  RP-tree:Forwarding:704441/639/782/3988, Other:704441/0/0
Group:239.0.18.133, Source count:0, Packets forwarded:8810, Packets received:8810
```

```
  RP-tree:Forwarding:8810/8/786/49, Other:8810/0/0
Group:239.0.18.193, Source count:0, Packets forwarded:0, Packets received:0
Group:239.0.17.193, Source count:0, Packets forwarded:0, Packets received:0
Group:239.0.18.134, Source count:0, Packets forwarded:8803, Packets received:8803
  RP-tree:Forwarding:8803/8/774/49, Other:8803/0/0
```

Note The RP-tree field is displayed only for non-SSM groups that have a (*, G) entry and a positive packet received count.

The following is sample output from the **show ip mroute** command with the **count** and **terse** keywords:

```
Router# show ip mroute count terse
IP Multicast Statistics
4 routes using 2610 bytes of memory
3 groups, 0.33 average sources per group
```

The table below describes the significant fields shown in the displays.

Table 5: show ip mroute count Field Descriptions

Field	Description
Group:	Summary statistics for traffic on an IP multicast group G. This row is displayed only for non-SSM groups.
Forwarding Counts:	Statistics on the packets that are received and forwarded to at least one interface. **Note** There is no specific command to clear only the forwarding counters; you can clear only the actual multicast forwarding state with the **clear ip mroute**command. Issuing this command will cause interruption of traffic forwarding.
Pkt Count/	Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created.
Pkts per second/	Number of packets received and forwarded per second. On an IP multicast fast-switching platform, this number is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.

Field	Description
Kilobits per second	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Total/	Total number of packets received.
RPF failed/	Number of packets not forwarded due to a failed RPF or acceptance check (when bidir-PIM is configured).
Other drops (OIF-null, rate-limit etc)	Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the OIF list was empty or because the packets were discarded because of a configuration, such as **ip multicast rate-limit**, was enabled).
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For SSM range groups, the groups displayed after the Group output field are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Source count:	Number of (S, G) states for this group G. Individual (S, G) counters are detailed in the output field rows.
Packets forwarded:	The sum of the packets detailed in the Forwarding Counts fields for this IP multicast group G. This field is the sum of the RP-tree and all Source fields for this group G.
Packets received:	The sum of packets detailed in the Other counts fields for this IP multicast group G. This field is the sum of the Other counts and Pkt Count fields of the RP-tree and Source rows for this group G.

Field	Description
RP-tree:	Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that does not forward packets on the shared tree. These (*, G) groups are bidir-PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM dense mode (PIM-DM) and SSM range groups.
Source:	Counters for an individual (S, G) state of this group G. There are no (S, G) states for bidir-PIM groups.

Related Commands

Command	Description
clear ip mroute	Deletes entries from the mroute table.

show ip msdp count

To display the number of sources and groups originated in Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages and the number of SA messages from an MSDP peer in the SA cache, use the **show ip msdp count**command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **count** [*as-number*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
as-number	(Optional) The number of sources and groups originated in SA messages from the specified autonomous system number.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the number of SA messages from each MSDP peer in the SA cache.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720 only.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip msdp cache-sa-state** command must be configured for this command to have any output.

Examples

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

```
Router# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
 224.135.250.116: 24
 172.16.240.253: 3964
 172.16.253.19: 10
 172.16.170.110: 11
SA State per ASN Counters, <asn>: <# sources>/<# groups>
 Total entries: 4009
 ?: 192/98, 9: 1/1, 14: 107/57, 17: 7/5
 18: 4/3, 25: 23/17, 26: 39/27, 27: 2/2
 32: 19/7, 38: 2/1, 52: 4/4, 57: 1/1
 68: 4/4, 73: 12/8, 81: 19/1, 87: 9/6
 .
 .
 .
```

The table below describes the significant fields shown in the display.

Table 6: show ip msdp count Field Descriptions

Field	Description
224.135.250.116: 24	MSDP peer with IP address 224.135.250.116: 24 SA messages from the MSDP peer in the SA cache.
Total entries	Total number of SA entries in the SA cache.
9: 1/1	Autonomous system 9: 1 source/1 group.

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.

show ip msdp peer

To display detailed information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp peer**command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **peer** [*peer-address*| *peer-name*] [**accepted-sas**| **advertised-sas**]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about MSDP peers associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-address | *peer-name*	(Optional) Domain Name System (DNS) name or IP address of the MSDP peer for which information is displayed.
accepted -sas	(Optional) Displays information about Source-Active (SA) messages received by the MSDP peer.
advertised -sas	(Optional) Displays information about SA messages advertised to the MSDP peer.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified. The output was modified to display information about the Source Active (SA) message limit configured using the **ip msdp sa-limit** command.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720 only.
12.4(2)T	This command was modified. The output was modified to display whether an MSDP peer has message digest 5 (MD5) password authentication enabled.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Examples

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

```
Router# show ip msdp peer 224.135.250.116
MSDP Peer 224.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
 Connection status:
   State: Up, Resets: 9, Connection source: Loopback2 (228.69.199.17)
   Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
   Output messages discarded: 0
   Connection and counters cleared 1w2d     ago
 SA Filtering:
   Input (S,G) filter: none, route-map: none
   Input RP filter: none, route-map: none
   Output (S,G) filter: none, route-map: none
   Output RP filter: none, route-map: none
 SA-Requests:
   Input filter: none
   Sending SA-Requests to peer: disabled
 Peer ttl threshold: 0
 SAs learned from this peer: 32, SAs limit: 500
 Input queue size: 0, Output queue size: 0
```

The table below describes the significant fields shown in the display.

Table 7: show ip msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the IP address for the TCP local connection address.
Uptime (Downtime):	Days and hours the MSDP peer is up or down. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.

Field	Description
Messages sent/received:	Number of SA messages sent to the MSDP peer/number of SA messages received from the MSDP peer.
SA Filtering:	Information regarding access list filtering of SA input and output, if any.
SA-Requests:	Information regarding access list filtering of SA requests, if any.
SAs learned from this peer:	Number of SA messages from the MSDP peer in the SA cache.
SAs limit:	SA message limit for this MSDP peer.

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

show ip msdp sa-cache

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

show ip msdp [**vrf** *vrf-name*] **sa-cache** [*group-address*| *source-address*| *group-name*| *source-name*] [*group-address*| *source-address*| *group-name*| *source-name*] [*as-number*] [**rejected-sa [detail] [read-only]**]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address source-address group-name source-name	(Optional) Group address, source address, group name, or source name of the group or source about which (S, G) state information is displayed. If two addresses or names are specified, an (S, G) entry corresponding to those addresses is displayed. If only one group address is specified, all sources for that group are displayed. If no options are specified, the entire Source-Active (SA) cache is displayed.
as-number	(Optional) Autonomous system (AS) number from which the SA message originated.
rejected-sa	(Optional) Displays the most recently received and rejected MSDP SA messages.
detail	(Optional) Displays detailed information about the IP address of the MSDP peer that sent the SA message and the reason that the SA message was rejected.
read-only	(Optional) Checkpoints the rejected SA cache. Once checkpointed, the rejected SA cache is emptied.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, (S,G) state is cached.

Rejected SA messages are cached only if the ip msdp cache-rejected-sa command is configured.

Use the **show ip msdp sa-cache** with the optional **rejected-sa** keyword to display SA messages stored in the rejected SA cache. When the **detail** keyword is added to the command string, the output includes the IP address of the MSDP peer router that sent the SA message and the reason that the SA message was rejected.

When the optional **read-only** keyword is added to the command string, the router checkpoints the rejected SA cache, which ensures that a consistent snapshot of the rejected SA cache is displayed in the output. After being checkpointed, the rejected SA cache is cleared.

Note Checkpointing the rejected SA cache requires that the router make a second copy of the rejected SA cache, which could cause the command to fail if the router is low on memory.

When the optional **read-only** keyword is not added to the command string, the router displays rejected MSDP SA messages out of the active rejected SA cache, which could result in inconsistent display output if rejected SA message entries are overwritten by rejected SA message entries that are captured as the output is being processed for display.

Examples

The following is sample output from the **show ip msdp sa-cache**command:

```
Router# show ip msdp sa-cache
MSDP Source-Active Cache - 2398 entries
(172.16.41.33, 238.105.148.0), RP 172.16.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.16.112.8, 224.2.0.1), RP 192.168.200.65, MBGP/AS 10888, 00:03:21/00:02:38
(172.16.10.13, 227.37.32.1), RP 192.168.3.92, MBGP/AS 704, 05:22:20/00:03:32
(172.16.66.18, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.66.148, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.10.13, 227.37.32.2), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:01:31
(172.16.70.203, 224.2.236.2), RP 192.168.253.7, MBGP/AS 3582, 02:34:16/00:05:49
(172.18.42.104, 236.195.56.2), RP 192.168.3.92, MBGP/AS 704, 04:21:13/00:05:22
(172.16.10.13, 227.37.32.3), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:02:31
(172.18.15.43, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 6d09h/00:05:35
(172.18.15.111, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.21.45, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.15.75, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.18.15.100, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.16.10.13, 227.37.32.6), RP 192.168.3.92, MBGP/AS 704, 00:45:30/00:05:31
(172.18.41.33, 224.247.228.10), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.18.222.210, 224.2.224.13), RP 192.168.3.92, MBGP/AS 704, 01:51:53/00:05:22
(172.18.41.33, 229.231.124.13), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:33
```

```
(172.18.32.138, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
(172.18.75.244, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
```

The table below describes the significant fields shown in the display.

Table 8: show ip msdp sa-cache Field Descriptions

Field	Description
(172.16.41.33, 238.105.148.0)	Indicates that the first address (source) is sending to the second address (group).
RP 172.16.3.111	IP address of the Rendezvous point (RP) where the SA message originated.
MBGP/AS 704	Indicates that the RP from which the SA message originated is in AS 704 according to multiprotocol Border Gateway Protocol (BGP).
2d10h/00:05:33	The route has been cached for 2 days and 10 hours. If no SA message is received in 5 minutes and 33 seconds, the route will be removed from the SA cache.

The following is sample output from the **show ip msdp sa-cache** command with the **rejected**, **detail**, and **read-only** keywords specified:

```
Router# show ip msdp sa-cache rejected detail read-only
MSDP Rejected SA Cache
 35 rejected SAs received over 02:50:01, cache size: 50 entries
 Timestamp (source, group)
 2832.248, (10.10.10.4, 227.7.7.12), RP: 10.10.10.4, Peer: 10.10.10.4,
     Reason: sa-limit-exceeded
 2915.232, (10.10.10.8, 224.1.1.1), RP: 10.11.11.11, Peer: 10.10.10.8,
     Reason: in-filter
 3509.584, (10.12.12.2, 225.5.5.5), RP: 10.15.15.1, Peer: 10.12.12.2,
           Reason: rpf-fail
 .
 .
 .
```

The table below describes the significant fields shown in the display.

Table 9: show ip msdp sa-cache rejected detail read-only Field Descriptions

Field	Description
35 rejected SAs received over 02:50:01	The number of rejected SA message entries received in the length of time indicated in HH:MM:SS.
cache size:	Indicates the size of the rejected SA cache. This field is controlled by the **ip msdp rejected-sa-cache** command. If the rejected SA cache overflows, entries are overwritten, starting from the first entry.
Timestamp	Indicates the router uptime in *seconds .milliseconds*.

Field	Description
(source, group)	The (S, G) information advertised in the rejected SA message.
RP:	Indicates the IP address of the Rendezvous Point (RP) that originated the SA message.
Peer:	Indicates the IP address of the MSDP peer that sent the rejected SA message.
Reason:	Indicates the reason that the router rejected the SA message. The possible reasons are as follows: • autorp-group--Indicates that the SA message was rejected because it included one of the two AutoRP groups (224.0.1.39 and 224.0.1.40). • in-filter--Indicates that the SA message was rejected because it was filtered by a configured incoming filter list (configured by the **ip msdp sa-filter in** command). • no-memory--Indicates that the SA message was rejected because the router ran out of memory while allocating storage for the MSDP SA message. • rpf-fail--Indicates that the SA message was rejected because it failed the Reverse Path Forwarding (RPF) check. • rp-filter--Indicates that the SA message was rejected because it was filtered by a configured incoming RP filter list (configured by the **ip msdp sa-filter in** command). • sa-limit-exceeded--Indicates that the SA message was rejected because the maximum number of SA cache entries (controlled by the **ip msdp sa-limit** command) was already exhausted when the SA message was received. • ssm-range--Indicates that the SA message was rejected because it indicated a group in the SSM range.

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP SA cache entries.
ip msdp cache-sa-state	Enables the router to create SA state.

show ip msdp summary

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

show ip msdp [**vrf** *vrf-name*] **summary**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the number of Source-Active (SA) messages from each MSDP peer in the SA cache.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Examples

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

```
Router# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
224.135.250.116  109   Up       1d10h    9     111   rtp5-rp1
*172.20.240.253 1239  Up       14:24:00 5     4010  sl-rp-stk
172.16.253.19    109   Up       12:36:17 5     10    shinjuku-rp1
172.16.170.110   109   Up       1d11h    9     12    ams-rp1
```

The table below describes the significant fields shown in the display.

Table 10: show ip msdp summary Field Descriptions

Field	Description
Peer Address	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State	State of the MSDP peer.
Uptime/Downtime	Days and hours the MSDP peer is up or down, per state shown in the previous column. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.
SA Count	Number of SA messages from this MSDP peer in the SA cache.
Peer Name	Name of the MSDP peer.

show ip pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **interface** [*type number*] [**df**| **count**] [*rp-address*] **[detail] [stats]**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about PIM interfaces associated with the Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name*argument.
type number	(Optional) Interface type and number.
df	(Optional) When bidirectional PIM (bidir-PIM) is used, displays the IP address of the elected designated forwarder (DF) for each rendezvous point (RP) of an interface.
count	(Optional) Specifies the number of packets received and sent out the interface.
rp-address	(Optional) RP IP address.
detail	(Optional) Displays PIM details of each interface.
stats	(Optional) Displays multicast PIM interface octet counts.

Command Default

If no interface is specified, all interfaces are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	This command was integrated into Cisco IOS Release 11.2(11)GS.
12.0(5)T	This command was modified. The flag “H” was added in the output display to indicate that an outgoing interface is hardware-switched in the case of IP multicast Multilayer Switching (MMLS).

Release	Modification
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.1(2)T	This command was modified. The **df** keyword and *rp-address* argument were added.
12.1(5)T	This command was modified. The **detail** keyword was added.
12.0(22)S	This command was modified. The command output changed to show when the query interval is set to milliseconds.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)S	This command was modified. The **stats** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(17)	This command was modified. The **stats** keyword was added.
12.4(7)	This command was modified. The **stats** keyword was added.
12.4(6)T	This command was modified. The **stats** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was modified. The “FS” column was removed from the output of the **show ip pim interface count** command due to the introduction of the IPv4 MFIB architecture.
15.0(1)M	This command was modified. The “FS” column was removed from the output of the **show ip pim interface count** command due to the introduction of the IPv4 MFIB architecture.
12.2(33)SRE	This command was modified. The “FS” column was removed from the output of the **show ip pim interface count** command due to the introduction of the IPv4 MFIB architecture.

Usage Guidelines

Use the **show ip pim interface count** command to display switching counts for Multicast Distributed Switching (MDS) and other switching statistics.

Note In Cisco IOS releases that support the IPv4 Multicast Forwarding Information Base (MFIB), use the **show ip mfib interface**command to display MFIB-related information about interfaces and their forwarding status.

Examples

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

```
Router# show ip pim interface
Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
10.1.0.1         GigabitEthernet0/0       v2/SD  0      30     1      10.1.0.1
10.6.0.1         GigabitEthernet0/1       v2/SD  1      30     1      10.6.0.2
10.2.0.1         ATM1/0.1                 v2/SD  1      30     1      0.0.0.0
```

The following is sample output from the **show ip pim interface** command when an interface is specified:

```
Router# show ip pim interface Ethernet1/0
Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       Ethernet1/0              v2/S   1      100 ms 1      172.16.1.4
```

The following is sample output from the **show ip pim interface** command when the **count** keyword is specified:

```
Router# show ip pim interface count
Address          Interface          FS  Mpackets In/Out
172.16.121.35    Ethernet0          *   548305239/13744856
172.16.121.35    Serial0.33         *   8256/67052912
192.168.12.73    Serial0.1719       *   219444/862191
```

The following is sample output from the **show ip pim interface** command when the **count**keyword is specified and IP MMLS is enabled. The example lists the PIM interfaces that are fast switched and process switched, and the packet counts for these interfaces. The H flag is added to interfaces where IP MMLS is enabled.

```
Router# show ip pim interface count
States: FS - Fast Switched, H - Hardware Switched
Address          Interface          FS  Mpackets In/Out
192.168.10.2       Vlan10             * H 40886/0
192.168.11.2       Vlan11             * H 0/40554
192.168.12.2       Vlan12             * H 0/40554
192.168.23.2       Vlan23             *   0/0
192.168.24.2       Vlan24             *   0/0
```

The following are two sample outputs from the **show ip pim interface** command when the **df** keyword is specified:

```
Router# show ip pim interface df
Interface          RP               DF Winner        Metric          Uptime
Ethernet3/3        10.10.0.2        10.4.0.2         0               00:03:49
                   10.10.0.3        10.4.0.3         0               00:01:49
                   10.10.0.5        10.4.0.4         409600          00:01:49
Ethernet3/4        10.10.0.2        10.5.0.2         0               00:03:49
                   10.10.0.3        10.5.0.2         409600          00:02:32
                   10.10.0.5        10.5.0.2         435200          00:02:16
Loopback0          10.10.0.2        10.10.0.2        0               00:03:49
                   10.10.0.3        10.10.0.2        409600          00:02:32
                   10.10.0.5        10.10.0.2        435200          00:02:16
Router# show ip pim interface Ethernet3/3 df 10.10.0.3
Designated Forwarder election for Ethernet3/3, 10.4.0.2, RP 10.10.0.3
  State                          Non-DF
  Offer count is                 0
  Current DF ip address          10.4.0.3
  DF winner up time              00:02:33
  Last winner metric preference  0
  Last winner metric             0
```

The table below describes the significant fields shown in the displays.

Table 11: show ip pim interface Field Descriptions

Field	Description
Address	Interface IP address of the next hop router.
Interface	Interface type and number that is configured to run PIM.
Ver/Mode	PIM version and multicast mode in which the Cisco IOS software is operating.
Nbr Count	Number of PIM neighbors that have been discovered through this interface. If the Neighbor Count is 1 for a DVMRP tunnel, the neighbor is active (receiving probes and reports).
Query Interval	Frequency, in seconds, of PIM hello messages, as set by the **ip pim query-interval** interface configuration command. The default is 30 seconds.
DR	IP address of the designated router (DR) on a network. **Note** Point-to-point interfaces do not have designated routers, so the IP address would be shown as 0.0.0.0.
FS	An asterisk (*) in this column indicates that fast switching is enabled.
Mpackets In/Out	Number of packets into and out of the interface since the router has been up.
RP	IP address of the RP.
DF Winner	IP address of the elected DF.
Metric	Unicast routing metric to the RP announced by the DF.
Uptime	Length of time the RP has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.
State	Indicates whether the specified interface is an elected DF.
Offer count is	Number of PIM DF election offer messages that the router has sent out the interface during the current election interval.

Field	Description
Current DF ip address	IP address of the current DF.
DF winner up time	Length of time the current DF has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.
Last winner metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the DF.
Last winner metric	Unicast routing metric to the RP announced by the DF.

The following is sample output from the **show ip pim interface** command with the **detail**keyword for Fast Ethernet interface 0/1:

```
Router# show ip pim interface fastethernet 0/1 detail
FastEthernet0/1 is up, line protocol is up
  Internet address is 172.16.8.1/24
  Multicast switching:process
  Multicast packets in/out:0/0
  Multicast boundary:not set
  Multicast TTL threshold:0
  PIM:enabled
    PIM version:2, mode:dense
    PIM DR:172.16.8.1 (this system)
    PIM neighbor count:0
    PIM Hello/Query interval:30 seconds
 PIM State-Refresh processing:enabled
 PIM State-Refresh origination:enabled, interval:60 seconds
    PIM NBMA mode:disabled
    PIM ATM multipoint signalling:disabled
    PIM domain border:disabled
  Multicast Tagswitching:disabled
```

The table below describes the significant fields shown in the display.

Table 12: show ip pim interface detail Field Descriptions

Field	Description
Internet address	IP address of the specified interface.
Multicast switching:	The type of multicast switching enabled on the interface: process, fast, or distributed.
Multicast boundary:	Indicates whether an administratively scoped boundary is configured.
Multicast TTL threshold:	The time-to-live (TTL) threshold of multicast packets being forwarded out the interface.
PIM:	Indicates whether PIM is enabled or disabled.

Field	Description
PIM version:	Indicates whether PIM version 1 or version 2 is configured.
mode:	Indicates whether PIM sparse mode, dense mode, or sparse-dense mode is configured.
PIM DR:	The IP address of the DR.
PIM State-Refresh processing:	Indicates whether the processing of PIM state refresh control messages is enabled.
PIM State-Refresh origination:	Indicates whether the origination of the PIM state refresh control messages is enabled.
interval:	Indicates the configured interval for the origination of the PIM state refresh control messages. The available interval range is from 4 to 100 seconds.
PIM NBMA mode:	Indicates whether the interface is enabled for nonbroadcast multiaccess (NBMA) mode.
PIM ATM multipoint signalling:	Indicates whether the interface is enabled for ATM multipoint signaling.
PIM domain border:	Indicates whether the interface is enabled as a PIM domain border.
Multicast Tagswitching:	Indicates whether multicast tag switching is enabled.

The following is sample output from the **show ip pim interface** command when the **stats** keyword is specified:

```
Router# show ip pim interface stats
Interface        Mpackets In    Mpackets Out         Octets In        Octets Out
Loopback0                  0               0                 0                 0
Loopback1                  0               0                 0                 0
Ethernet0/0                0               0                 0                 0
Ethernet0/3                0               0                 0                 0
Ethernet1/1                0               0                 0                 0
```

For all of the count descriptions, a packet is counted as a multicast packet if either of the following two conditions is met:

- The IP address contained in the IP header of the packet specifies a multicast (class D) IP address.
- The IP address contained in the IP header of the packet specifies an IP address located on this router and the packet contains an encapsulated packet for which the IP header of the encapsulated packet specifies a multicast (class D) IP address.

The table below describes the significant fields shown in the display.

Table 13: show ip pim interface stats Field Descriptions

Field	Description
Mpackets In	The number of multicast packets received on each interface listed in the output.
Mpackets Out	The number of multicast packets sent on each interface listed in the output.
Octets In	Cumulative byte count for data bytes (including IP header bytes) contained within multicast packets received on each interface listed in the output.
Octets Out	Cumulative byte count for data bytes (including IP header bytes) contained within multicast packets sent on each interface listed in the output.

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim query-interval	Configures the frequency of PIM router query messages.
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh control messages on a PIM router.
ip pim state-refresh origination-interval	Configures the origination of and the interval for PIM dense mode state refresh control messages on a PIM router.
show ip mfib interface	Displays MFIB-related information about interfaces and their forwarding status.
show ip pim neighbor	Displays information about PIM neighbors.

show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp**command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp** [**mapping**| **metric**] [*rp-address*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mapping	(Optional) Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP).
metric	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
rp-address	(Optional) RP IP address.

Command Default

If no RP is specified, all active RPs are displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.1(2)T	The **metric** keyword and *rp-address* argument were added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Protocol Independent Multicast (PIM) version known for an RP influences the type of PIM register messages (Version 1 or Version 2) that the router sends when acting as the designated router (DR) for an active source. If an RP is statically configured, the PIM version of the RP is not set and the router, if required to send register packets, tries to send PIM Version 2 register packets. If sending PIM Version 2 packets fails, the router sends PIM Version 1 register packets.

The version of the RP displayed in the **show ip pim rp** command output can change according to the operations of the router. When the group is created, the version shown is for the RP in the RP mapping cache. Later, the version displayed by this command may change. If this router is acting as a DR for an active source, the router sends PIM register messages. The PIM register messages are answered by the RP with PIM register stop messages. The router learns from these PIM register stop messages the actual PIM version of the RP. Once the actual PIM version of the RP is learned, this command displays only this version. If the router is not acting as a DR for active sources on this group, then the version shown for the RP of the group does not change. In this case, the PIM version of the RP is irrelevant to the router because the version of the RP influences only the PIM register messages that this router must send.

When you enter the **show ip pim rp mapping** command, the version of the RP displayed in the output is determined only by the method through which an RP is learned. If the RP is learned from Auto-RP then the RP displayed is either “v1” or “v2, v1.” If the RP is learned from a static RP definition, the RP version is undetermined and no RP version is displayed in the output. If the RP is learned from the BSR, the RP version displayed is “v2.”

Examples

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

```
Router# show ip pim rp
Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

The following is sample output from the **show ip pim rp**command when the **mapping** keyword is specified:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
         Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
         Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
Group(s) (-)230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
```

The following is sample output from the **show ip pim rp**command when the **metric** keyword is specified:

```
Router# show ip pim rp metric
RP Address      Metric Pref    Metric       Flags   RPF Type   Interface
10.10.0.2       0              0              L     unicast    Loopback0
10.10.0.3       90             409600         L     unicast    Ethernet3/3
10.10.0.5       90             435200         L     unicast    Ethernet3/3
```

The table below describes the significant fields shown in the displays.

Table 14: show ip pim rp Field Descriptions

Field	Description
Group	Address of the multicast group about which to display RP information.
RP	Address of the RP for that group.
v2	Indicates that the RP is running PIM version 2.
v1	Indicates that the RP is running PIM version 1.
bidir	Indicates that the RP is operating in bidirectional mode.
Info source	RP mapping agent that advertised the mapping.
(?)	Indicates that no Domain Name System (DNS) name has been specified.
via Auto-RP	Indicates that RP was learned via Auto-RP.
Uptime	Length of time the RP has been up (in days and hours). If less than 1 day, time is shown in hours, minutes, and seconds.
expires	Time in (hours, minutes, and seconds) in which the entry will expire.
Metric Pref	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.
Flags	Indicates the flags set for the specified RP. The following are descriptions of possible flags: • C--RP is configured. • L--RP learned via Auto-RP or the BSR.

Field	Description
RPF Type	Routing table from which this route was obtained, either unicast, Distance Vector Multicast Routing Protocol (DVMRP), or static mroute.
Interface	Interface type and number that is configured to run PIM.

show ip rpf

To display the information that IP multicast routing uses to perform the Reverse Path Forwarding (RPF) check for a multicast source, use the **show ip rpf**command in user EXEC or privileged EXEC mode.

show ip rpf [**vrf** *vrf-name*] {*route-distinguisher*| *source-address* [*group-address*] [**rd** *route-distinguisher*]} **[metric]**

Cisco ASR 1000 Series

show ip rpf [**vrf** *vrf-name*] *source-address* [*group-address*] [**rd** *route-distinguisher*] **[metric]**

Syntax Description

vrf *vrf-name*	(Optional) Displays the information that IP multicast routing uses to perform the RPF check for a multicast source associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name*argument.
route-distinguisher	Route distinguisher (RD) of a VPNv4 prefix. Entering the *route-distinguisher* argument displays RPF information related to the specified VPN route. You can enter an RD in either of these formats: • 16-bit autonomous system (AS) number: your 32-bit number, for example, 101:3 • 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1
source-address	IP address or name of a multicast source for which to display RPF information.
group-address	(Optional) IP address or name of a multicast group for which to display RPF information.
rd *route-distinguisher*	(Optional) Displays the Border Gateway Protocol (BGP) RPF next hop for the VPN route associated with the RD specified for the *route-distinguisher* argument. You can enter an RD in either of these formats: • 16-bit autonomous system (AS) number: your 32-bit number, for example, 101:3 • 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1
metric	(Optional) Displays the unicast routing metric.

Command Modes User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.1(2)T	This command was modified. The **metric** keyword was added.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(29)S	This command was modified. The *group-address*argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The *group-address*argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
12.2(31)SB2	This command was modified. The output was modified to indicate that the Multicast VPN Extranet VRF Select feature is being used to perform the RPF lookup based on the group address and the VRF where the RPF lookup is being performed.
12.2(33)SXH	This command was modified. The *group-address*argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
12.4(20)T	This command was modified. The *group-address*argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
15.0(1)M	This command was modified. The output was modified to indicate that the Multicast VPN Extranet VRF Select feature is being used to perform the RPF lookup based on the group address and the VRF where the RPF lookup is being performed.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.

Release	Modification
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **show ip rpf** command to display the information that IP multicast routing uses to perform the Reverse Path Forwarding (RPF) check for a multicast source. When performing the RPF calculation, the router can use multiple routing tables (the unicast routing table, Multiprotocol Border Gateway Protocol (MBGP) table, Distance Vector Multicast Routing Protocol [DVMRP] routing table, or static multicast routes) to determine the interface on which traffic from a source should arrive (the RPF interface). Because the RPF check can be performed from multiple routing tables, the **show ip rpf**command can be used to identify the source of the retrieved information.

In a Multi-Topology Routing (MTR) routing environment, a router can perform RPF lookups from multiple unicast Routing Information Bases (RIBs)--instead of only looking at the original unique unicast RIB. By default, the Cisco IOS software supports the pre-MTR IP multicast behavior; that is, the RPF check is performed on routes in the unicast RIB (base unicast topology).

Note MTR introduces a multicast topology (base multicast topology) that is completely independent from the unicast topology. MTR integration with multicast allows the path of multicast traffic to be controlled in the network.

Examples

The following is sample output from the **show ip rpf**command:

```
Router# show ip rpf 172.16.10.13
RPF information for host1 (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: sj1.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

The following is sample output from the **show ip rpf** command with the optional **vrf** keyword, *vrf-name* argument, and *group-address* argument:

```
Router# show ip rpf vrf green 10.1.1.100 232.6.6.6
RPF information for ? (10.1.1.100)
  RPF interface: Ethernet3/0
  RPF neighbor: ? (10.1.1.5)
  RPF route/mask: 10.1.1.0/24
  RPF type: unicast (rip)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Using Group Based VRF Select, RPF VRF: blue
```

The following is sample output from the **show ip rpf**command with the **metric** keyword:

```
Router# show ip rpf 172.16.10.13 metric
RPF information for host1.cisco.com (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: neighbor.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
```

```
  Doing distance-preferred lookups across tables
  Metric preference: 110
  Metric: 11
```

The following is sample output from the **show ip rpf** command in an MTR routing environment. In Cisco IOS releases that support MTR, the "RPF topology" field was introduced to indicate which RIB topology is being used for the RPF lookup. For the "RPF topology" field in this example, the first topology listed (ipv4 multicast base) indicates where the nexthop of the RPF lookup is being conducted and the second topology listed (ipv4 unicast data) indicates where the route originated from.

```
Router# show ip rpf 10.30.30.32
RPF information for ? (10.30.30.32)
  RPF interface: Ethernet1/0
  RPF neighbor: ? (10.1.1.32)
  RPF route/mask: 10.30.30.32/32
  RPF type: unicast (ospf 100)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base, originated from ipv4 unicast data
```

The table below describes the fields shown in the displays.

Table 15: show ip rpf Field Descriptions

Field	Description
RPF information for	Hostname and source address for which RPF information is displayed.
RPF interface	For the given source, the interface from which the router expects to receive packets.
RPF neighbor	For the given source, the neighbor from which the router expects to receive packets.
RPF route/mask	Route number and mask that matched against this source.
RPF type	Routing table from which this route was obtained, either unicast, MBGP, DVMRP, or static mroutes.
RPF recursion count	The number of times the route is recursively resolved.
Doing distance-preferred	Whether RPF was determined based on distance or length of mask.
Using Group Based VRF Select, RPF VRF:	The RPF lookup was based on the group address and the VRF where the RPF lookup is being performed.
Metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.

Field	Description
RPF topology	RIB topology being used for the RPF lookup, and, if originated from a different RIB topology, which RIB topology the route originated from.

The following is sample output from the **show ip rpf** command in a Multicast only Fast Re-Route (MoFRR) enabled environment. The command output shows that MoFRR is enabled for the 209.165.200.226 multicast source IP address. The relevant command output is shown in bold.

```
Router# show ip rpf 209.165.200.226
RPF information for ? (209.165.200.226) MoFRR Enabled
  RPF interface: Ethernet1/4
  RPF neighbor: ? (209.165.201.2)
  RPF route/mask: 255.255.255.225
  RPF type: unicast (ospf 200)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base, originated from ipv4 unicast base
  Secondary RPF interface: Ethernet1/3
  Secondary RPF neighbor: ? (209.165.202.128)
```

The table below describes the fields shown in the displays.

Table 16: show ip rpf Command Output in an MoFRR-Enabled Environment: Field Descriptions

Field	Description
RPF information for	Hostname and source address for which RPF information is displayed, including MoFRR status.
RPF interface	For the given source, the interface from which the router expects to receive packets.
RPF neighbor	For the given source, the neighbor from which the router expects to receive packets.
RPF route/mask	Route number and mask that matched against this source.
RPF type	Routing table from which this route was obtained, either unicast, MBGP, DVMRP, or static mroutes.
Doing distance preferred	Whether RPF was determined based on distance or length of mask.
RPF topology	RIB topology being used for the RPF lookup, and, if originated from a different RIB topology, which RIB topology the route originated from.
Secondary RPF interface	For the given source, the secondary interface from which the router expects to receive packets.

Field	Description
Secondary RPF neighbor	For the given source, the secondary neighbor from which the router expects to receive packets.

show ip rpf events

To display the last 15 triggered multicast Reverse Path Forwarding (RPF) check events, use the **show ip rpf events**command in user EXEC or privileged EXEC mode.

show ip rpf [**vrf** *vrf-name*] **events**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to determine the most recent triggered multicast RPF check events.

Examples

The following is sample output from the **show ip rpf events**command:

```
Router# show ip rpf events
Last 15 triggered multicast RPF check events
RPF backoff delay:500 msec
RPF maximum delay:5 sec
DATE/TIME            BACKOFF    PROTOCOL   EVENT         RPF CHANGES
Mar 7 03:24:10.505    500 msec   Static     Route UP        0
Mar 7 03:23:11.804    1000 sec   BGP        Route UP        3
Mar 7 03:23:10.796    500 msec   ISIS       Route UP        0
Mar 7 03:20:10.420    500 msec   ISIS       Route Down      3
Mar 7 03:19:51.072    500 msec   Static     Route Down      0
```

```
Mar 7 02:46:32.464    500 msec   Connected  Route UP        3
Mar 7 02:46:24.052    500 msec   Static     Route Down      0
Mar 7 02:46:10.200    1000 sec   Connected  Route UP        3
Mar 7 02:46:09.060    500 msec   OSPF       Route UP        3
Mar 7 02:46:07.416    500 msec   OSPF       Route Down      0
Mar 7 02:45:50.423    500 msec   EIGRP      Route UP        3
Mar 7 02:45:09.679    500 msec   EIGRP      Route Down      0
Mar 7 02:45:06.322    500 msec   EIGRP      Route Down      2
Mar 7 02:33:09.424    500 msec   Connected  Route UP        0
Mar 7 02:32:28.307    500 msec   BGP        Route UP        3
```

The following is sample output from the **show ip rpf events**command when the **ip multicast rpf backoff** command is used with the **disable** keyword, disabling the triggered RPF check function:

```
Router# show ip rpf events
Last 15 triggered multicast RPF check events
Note:Triggered RPF disabled!
RPF backoff delay:50 msec
RPF maximum delay:2 sec
DATE/TIME             BACKOFF    PROTOCOL   EVENT         RPF CHANGES
Sep 4 06:25:31.707    500 msec   Connected  Route UP        0
Sep 4 06:25:30.099    500 msec   Connected  Route UP        0
```

The table below describes the significant fields shown in the display.

Table 17: show ip rpf events Field Descriptions

Field	Description
RPF backoff delay	The configured amount of time (in milliseconds) allowed for the initial backoff delay.
RPF maximum delay	The maximum configured amount of time (in seconds) allowed for a backoff delay.
DATE/TIME	The date and time (in hours:minutes:seconds) an RPF event occurred.
BACKOFF	The actual backoff delay (in milliseconds) after which the RPF check was done.
PROTOCOL	The protocol that triggered the RPF check.
EVENT	This RPF check was caused by a route that went up or down, or was modified.
RPF CHANGES	The number of multicast routes that were affected by the RPF change.

show ipv6 mld snooping

To display Multicast Listener Discovery version 2 (MLDv2) snooping information, use the **show ipv6 mld snooping** command in privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **snooping** {**explicit-tracking vlan** *vlan*| **mrouter** [**vlan** *vlan*]| **report-suppression vlan** *vlan*| **statistics vlan** *vlan*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
explicit-tracking vlan *vlan*	Displays the status of explicit host tracking.
mrouter	Displays the multicast router interfaces on an optional VLAN.
vlan *vlan*	(Optional) Specifies the VLAN number on the multicast router interfaces.
report-suppression vlan *vlan*	Displays the status of the report suppression.
statistics vlan *vlan*	Displays MLD snooping information on a VLAN.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

You can enter the **show ipv6 mld snooping mrouter** command without arguments to display all the multicast router interfaces.

Examples

This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
-------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show
ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
```

This example shows the MLD snooping statistics information for VLAN 25:

```
Router# show ipv6 mld
 snooping statistics interface vlan 25
Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
```

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 snooping globally.
ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
ipv6 mld snooping querier	Enables the MLDv2 snooping querier.
ipv6 mld snooping report-suppression	Enables report suppression on a VLAN.

snmp-server enable traps pim

To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim**command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no**form of this command.

snmp-server enable traps pim [**neighbor-change**| **rp-mapping-change**| **invalid-pim-message**]

no snmp-server enable traps pim

Syntax Description

neighbor-change	(Optional) Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires.
rp-mapping-change	(Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
invalid-pim-message	(Optional) Enables invalid PIM message traps. For example, an invalid PIM message could result when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface on the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
Router(config)# snmp-server host 10.0.0.1 traps version 2c public pim

! Configure router to send the neighbor-change class of notifications to host.
Router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
Router(config)# interface ethernet0/0

Router(config-if)# ip pim sparse-dense-mode
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.