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.