show ip dvmrp route through show ip sdr

show ip dvmrp route

Note The **show ip dvmrp route**command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To display the contents of the Distance Vector Multicast Routing Protocol (DVMRP) routing table, use the **show ip dvmrp route** command in user EXEC or privileged EXEC mode.

show ip dvmrp route [**address** *hostname*| **interface** *type number*] **[poison]**

Syntax Description

address	(Optional) Displays information about the specified DVMRP route.
hostname	(Optional) IP name or IP address.
interface	(Optional) Displays information about the specified interface from the DVMRP routing table.
type	(Optional) Interface type.
number	(Optional) Interface or subinterface number.
poison	(Optional) Displays information about DVMRP routes that have been poisoned.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA and the **poison** keyword was added.
12.2(33)SRB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **show ip dvmrp route** EXEC command to show the contents of the DVMRP routing table.

Examples

The following example shows output of the **show ip dvmrp route**command:

```
Router# show ip dvmrp route
DVMRP Routing Table - 1 entry
172.16.0.0/16 [100/11] uptime 07:55:50, expires 00:02:52
    via 192.168.0.0, Tunnel3
```

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

Table 1: show ip dvmrp route Field Descriptions

Field	Description
1 entry	Number of entries in the DMVRP routing table.
172.16.0.0/16	Source network.
[100/11]	Administrative distance/metric.
uptime	How long (in hours, minutes, and seconds) that the route has been in the DVMRP routing table.
expires	How long (in hours, minutes, and seconds) until the entry is removed from the DVMRP routing table.
via 192.168.0.0	Next hop router to the source network.
Tunnel3	Interface to the source network.

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 2: 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 3: 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 membership

To display Internet Group Management Protocol (IGMP) membership information for multicast groups and (S, G) channels, use the **show ip igmp membership** command in user EXEC or privileged EXEC mode.

show ip igmp membership [*group-address*| *group-name*] **[tracked] [all]**

Syntax Description

group-address	(Optional) The IP address of the multicast group for which to display IGMP membership information.
group-name	(Optional) The name of the multicast group, as defined in the Domain Name System (DNS) hosts table, for which to display IGMP membership information.
tracked	(Optional) Displays the multicast groups with the explicit tracking feature enabled.
all	(Optional) Displays the detailed information about the multicast groups with and without the explicit tracking feature enabled.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(19)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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

Use this command to display IGMP membership information for multicast groups and (S, G) channels. This command allows you to display detailed information about multicast group and channel membership and explicit tracking.

Examples

The following is sample output from the **show ip igmp membership** user EXEC command. Each entry in the output shows the aggregate membership information (indicated by the A flag) for a particular multicast group or channel from the IGMP cache. If the entry is prepended with a forward slash ("/") flag, the entry is a filtering entry that is blocking the data forwarding of the multicast group or channel.

```
Router> show ip igmp membership
Flags:A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, D - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode,<m> reporter in exclude
 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,224.0.1.40                  10.10.0.1       00:01:34 02:41 2LA   Et2/0
 *,239.1.1.1                   2/0             00:00:10 stop  3AT    Et2/0
```

The following is sample output from the **show ip igmp membership** user EXEC command with the multicast group address 239.1.1.1 and the **tracked** keyword specified:

```
Router> show ip igmp membership 239.1.1.1 tracked
Flags:A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, D - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode,<m> reporter in exclude
 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,239.1.1.1                   2/0             00:00:11 stop  3AT    Et2/0
 10.30.0.100,239.1.1.1         10.10.0.10      00:00:11 02:48 RT     Et2/0
 10.30.0.101,239.1.1.1         10.10.0.20      00:00:03 02:56 RT     Et2/0
 10.30.0.101,239.1.1.1         10.10.0.10      00:00:11 02:48 RT     Et2/0
 10.30.0.102,239.1.1.1         10.10.0.20      00:00:03 02:56 RT     Et2/0
```

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

Table 4: show ip igmp membership Field Descriptions

Field	Description
Channel/Group	(S, G) channel or multicast group filtering entry.
Reporter	Displays information about the hosts reporting membership with the (S, G) channel or multicast group entry.
Uptime	The Uptime timer is how long (in hours, minutes, and seconds) the entry has been known.
Exp.	The Exp. timer is how long (in minutes and seconds) until the entry expires.

Field	Description
Flags	Provides information about the entry: • A--aggregate. Indicates that the aggregate information for the (S, G) channel or multicast group is being displayed. • T--tracked--Indicates that the multicast group is configured with the explicit tracking feature. • L--local. Indicates that the router itself is interested in receiving the traffic for this multicast group or channel. In order for the application to receive this traffic, the packets are sent to the process level of the router. When the **ip igmp join-group** command is configured for a multicast group, the L flag is set. • S--static. Indicates that the multicast group or channel is forwarded on the interface. When the **ip igmp static-group**command is configured on the interface, the S flag is set. • V--virtual. Indicates that service such as Hoot and Holler is running on the router requesting the traffic for the multicast group or channel. These services can process IP multicast traffic in the fast switching path. The L flag will not be set by these applications.
	• R--reported through v3. Indicates that an IGMP Version 3 (IGMPv3) report was received for this entry. • I--v3lite. Indicates that an IGMP Version 3 lite (IGMP v3lite) report was received for this entry. • D--URD. Indicates that a URL Rendezvous Directory (URD) report was received for this entry. • M--SSM (S, G) channel. Indicates that the multicast group address is in the Source Specific Multicast (SSM) range. • 1, 2, 3--The version of IGMP. The version of IGMP that the multicast group is running.
Interface	Interface type and number.

Related Commands

Command	Description
ip igmp explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMP Version 3.
ip igmp version	Configures the version of IGMP that the router uses.
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

show ip igmp 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 explicit-tracking

To display the information about the explicit host-tracking status for IGMPv3 hosts, use the show ip igmp **snooping explicit-tracking**command in user EXEC or privileged EXEC mode.

show ip igmp snooping explicit-tracking vlan *vlan-id*

Syntax Description

vlan *vlan-id*	Specifies the VLAN to display.

Command Default

If you do not specify a VLAN, information for VLAN 1 is displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

:This example shows how to display the information about the explicit host-tracking status for all IGMPv2 and IGMPv3 hosts:

```
Router# show ip igmp snooping explicit-tracking
Current number of entries: 3 Configured DB size limit: 32000
VLAN 1
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 2
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 6
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 7
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 10
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
0.0.0.0/224.0.1.40 Vl10: 11.10.0.2 EXCLUDE
:
Router#
```

:This example shows how to display the information about the explicit host-tracking status for IGMPv2 and IGMPv3 hosts:

```
Router# show ip igmp 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
Router#
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit host tracking.

show ip igmp snooping filter

To display the Internet Group Management Protocol (IGMP) filtering rules, use the **show ip igmp snooping filter** command in privileged EXEC mode.

show ip igmp snooping filter interface *type mod*/*port* **[statistics]**

Syntax Description

interface *type*	Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number
statistics	(Optional) Displays IGMP filtering statistics.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

IGMP filtering allows you to configure filters on a per-port basis, a per-switch virtual interface (SVI) basis, or both.

The *mod* / *port* is not supported when you enter the **vlan** *vlan-id* keyword and argument.

IGMP filtering is supported for IPv4 only.

IGMP filters is not supported on routed ports.

If the port is in the shutdown state, the system cannot determine if the port is in trunk mode or access mode, and you will not be able to display the filter status by entering the **show ip igmp snooping filter** command. In this case, you can enter the **show running-config interface** command to display the configuration.

IGMP filtering statistics are maintained for the following only:

- A specific switch port in an SVI.
- A specific VLAN in a trunk.

Examples

The following example displays the default filters configured on the SVI:

```
Router# show ip igmp snooping filter interface vlan 20
Access-Group: Channel1-Acl
Groups/Channels Limit: 100 (Exception List: Channel6-Acl)
IGMP Minimum-Version: Not Configured
Router#
```

The following example displays the output on a switch port that is in access mode:

```
Router# show ip igmp snooping filter interface gigabitethernet3/48
Access-Group: Channel4-Acl
Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
Router#
```

The following example displays the filters configured for all switch ports in access mode under this SVI:

```
Router# show ip igmp snooping filter interface vlan 20 detail
VLAN20 :
Access-Group: Not Configured
Groups/Channels Limit: Not Configured
VLAN20 :
Access-Group: Channel4-ACL
Groups/Channels Limit: 10 (Exception-list: Channel3-Acl)
Router#
```

The following example displays the default trunk port filters:

```
Router# show ip igmp snooping filter interface gigabitethernet3/46
Access-Group: Channel1-Acl
Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
Router#
```

The following example displays the per-VLAN filters for all VLANs on this trunk:

```
Router# show ip igmp snooping filter interface gigabitethernet3/46 detail
Vlan 10 :
Access-Group: Not Configured
Groups/Channels Limit: Not Configured
Vlan 20 :
Access-Group: Not Configured
Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
Router#
```

The following example displays the output on a trunk port for a specific VLAN:

```
Router# show ip igmp snooping filter interface gigabitethernet3/46 vlan 20
Access-Group: Not Configured
Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
Router#
```

The following example displays the statistics for each switch port in access mode under the SVI:

```
Router# show ip igmp snooping filter interface vlan 20 statistics
GigabitEthernet3/47 :
IGMP Filters are not configured
GigabitEthernet3/48 :
Access-group denied : 0
Limit denied : 2
Limit status : 0 active out of 2 max
Minimum-version denied : 0
```

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

Table 5: show ip igmp snooping Field Descriptions

Field	Description
Access-Group: Channel1-Acl	Name of the access group.
Groups/Channels Limit: 100 (Exception List: Channel6-Acl)	Number of IGMP groups or channels allowed on an interface is set to 100, with the exception of group Channel1-Acl.
IGMP Minimum-Version: Not Configured	Minimum version not configured (**ip igmp snooping minimum-version** command).
IGMP Filters are not configured	Filtering on the IGMP protocol is disabled.
Access-group denied : 0	Number of access groups denied.
Limit denied : 2	
Limit status : 0 active out of 2 max	Number of active groups.
Minimum-version denied : 0	

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
ip igmp snooping minimum-version	Filters on the IGMP protocol.

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 snooping rate-limit

To display the information about the IGMP-snooping rate limit, use the **show ip igmp snooping rate-limit** command in user EXEC or privileged EXEC mode.

show ip igmp snooping rate-limit [**statistics**| **vlan** *vlan-id*]

Syntax Description

statistics	(Optional) Displays IGMP-snooping statistics.
vlan *vlan-id*	(Optional) Specifies a VLAN; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the statistics for IGMP-snooping rate limiting:

```
Router#
 show ip igmp snooping rate-limit
 statistics
Max IGMP messages incoming rate : Not configured
Vlan   Incoming rate  Rate-limiting ON  Disable count  Time to Enable
-----+---------------+----------------+---------------+---------------+
222   1000            No                0
111   5999            Yes               3               185
```

This example shows how to display IGMP-snooping rate-limit information for a specific VLAN:

```
Router#
 show ip igmp snooping rate-limit vlan 19
Max IGMP messages incoming rate : 200 pps
Vlan       Incoming IGMP rate (in pps)
--------+---------------------------------
19       200
```

Related Commands

Command	Description
ip igmp snooping rate	Sets the rate limit for IGMP-snooping packets.

show ip igmp snooping statistics

To display IGMPv3 statistics, use the **show ip igmp snooping statistics**command in user EXEC or privileged EXEC mode.

show ip igmp snooping statistics {**interface** *type*[*number*]| **port-channel** *number*| **vlan** *vlan-id*}

Syntax Description

interface type	(Optional) Displays IGMP statistics for the specified interface type; possible valid values are **ethernet**, **fastethernet**, and **gigabitethernet**.
number	(Optional) Multicast-related statistics for the specified module and port; see the "Usage Guidelines" section for valid values.
port-channel *number*	(Optional) Displays multicast-related statistics for the specified port-channel; valid values are from 1 to 282.
vlan *vlan-id*	(Optional) Displays multicast-related statistics for the specified VLAN; valid values for *vlan-id*are from 1 to 4094 .

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **show ip igmp snooping statistics** command displays the following statistics:

- List of ports that are members of a group
- Filter mode
- Reporter-address behind the port
- Additional information (such as the last-join and last-leave collected since the previous time that a **clear ip igmp snooping statistics** command was issued)

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number*values from 257 to 282 are supported on the CSM and the FWSM only.

The #hosts behind the VLAN is displayed only if you define the max-hosts policy on the specified VLAN and enable the log policy for the specified VLAN.

Examples

This example shows how to display IGMPv3 statistics:

```
Router# show ip igmp snooping statistics interface FastEthernet5/1
IGMP Snooping statistics
Service-policy: Policy1policy tied with this interface
#Channels: 3
#hosts : 3
Query Rx: 2901 GS Query Rx: 0 V3 Query Tot Rx: 0
Join Rx: 8686 Leave Rx: 0 V3 Report Rx: 2300
Join Rx from router ports: 8684 Leave Rx from router ports: 0
Total Rx: 11587
Channel/Group         Interface  Reporter    Uptime     Last-Join  Last-Leave
10.7.20.1,239.1.1.1   F5/1       10.5.20.1   00:12:00   1:10:00    -
10.7.30.1,239.1.1.1   F5/1       10.5.30.1   00:50:10   1:10:02    0:30:02
10.7.40.1,239.1.1.1   F5/1       10.5.40.1   00:10:10   1:10:03    -
```

The table below describes the fields that are shown in the example.

Table 6: show ip igmp snooping statistics Field Descriptions

Field	Description
Service-policy: Policy1	Policy tied to this interface.
#Channels: 3	Number of channels behind the specified interface.
#hosts	Number of hosts behind the specified interface. This field is displayed only if max-hosts policy is used.

Related Commands

Command	Description
clear ip igmp snooping statistics	Clears the IGMP-snooping statistics.

show ip igmp ssm-mapping

To display information about Source Specific Multicast (SSM) mapping or to display the sources that SSM mapping uses for a particular group, use the **show ip igmp ssm-mapping** command in user EXEC or privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **ssm-mapping** [*group-address*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address	(Optional) Address of the group about which to display SSM mapping information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
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.

Usage Guidelines

Use this command to display the sources that SSM mapping is using for a particular group, or would use for a group if SSM mapping were configured. If no SSM mapping is known for the specified group, and Domain Name System (DNS)-based SSM mapping is enabled, this command sends out a DNS query for the group. The DNS query initiates DNS-based SSM mapping for this group. If no SSM mapping group is specified by the *group-address*argument, this command displays the configured SSM mapping state.

Use the **vrf** *vrf-name* keyword and argument to displays SSM mapping information for a particular VRF.

Examples

The following example shows how to display information about the configured SSM mapping state:

```
Router# show ip igmp ssm-mapping
SSM Mapping  : Enabled
DNS Lookup   : Enabled
Mcast domain : ssm-map.cisco.com
Name servers : 10.0.0.0
               10.0.0.1
```

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

Table 7: show ip igmp ssm-mapping Field Descriptions

Field	Description
SSM Mapping : Enabled	The SSM Mapping feature is enabled.
DNS Lookup : Enabled	DNS-based SSM mapping is enabled.
Mcast domain : ssm-map.cisco.com	Multicast domain.
Name servers : 10.0.0.0 10.0.0.1	Addresses of the configured named servers.

The following example shows how to display information about the configured DNS-based SSM mapping:

```
Router# show ip igmp ssm-mapping 232.1.1.4
Group address: 232.1.1.4
Database     : DNS
DNS name     : 4.1.1.232.ssm-map.cisco.com
Expire time  : 860000
Source list  : 172.16.8.5
              :172.16.8.6
```

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

Table 8: show ip igmp ssm-mapping Field Descriptions

Field	Description
Group address: 232.1.1.4	The router has mapped group 232.1.1.4.
Database : DNS	Group mapping is performed via DNS.
DNS name : 4.1.1.232.ssm-map.cisco.com	Name of the DNS that performs group mapping.
Expire time : 860000	Cache time of the DNS registration record on the DNS server, in milliseconds.
Source list : 172.16.8.5 :172.16.8.6	The group address is mapped via DNS to these source addresses.

The following example shows how to display information about the configured static SSM mapping:

```
Router# show ip igmp ssm-mapping 232.1.1.4
Group address: 232.1.1.4
Database     : Static
Source list  : 172.16.8.5
             : 172.16.8.6
```

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

Table 9: show ip igmp ssm-mapping Field Descriptions

Field	Description
Group address: 232.1.1.4	The address of the group with SSM mapping to the router.
Database : Static	Static SSM mapping is configured.
Source list : 172.16.8.5 : 172.16.8.6	Source addresses configured for static SSM mapping.

The following is sample output from the **show ip igmp ssm-mapping** command when no SSM mappings can be found:

```
Router# show ip igmp ssm-mapping 232.1.1.4
Can't resolve %i to source-mapping
```

Related Commands

Command	Description
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
show ip igmp group	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

show ip igmp static-group class-map

To display the contents of Internet Group Management Protocol (IGMP) static group class map configurations and the interfaces using class maps, use the **show ip igmp static-group class-map** command in user EXEC or privileged EXEC mode.

show ip igmp static-group class-map [**interface** [*type number*]]

Syntax Description

interface	(Optional) Filters the output to display only the interfaces using class maps.
type number	(Optional) Interface type and number entered to filter the output to display only the class map attached to a particular interface.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use this command to display the contents of IGMP static group class map configurations and the interfaces using class maps.

Use this command with the optional **interface** keyword to filter the output to display only the interfaces using class maps.

Use this command with the optional **interface** keyword and *type number* arguments to filter the output to display only the class map attached to a particular interface.

Examples

The following is sample output from the **show ip igmp static-group class-map** command. The output is self-explanatory:

```
Router# show ip igmp static-group class-map
Class-map static1
  Group address range 228.8.8.7 to 228.8.8.9
  Group address 232.8.8.7, source address 10.1.1.10
  Interfaces using the classmap:
    Loopback0
Class-map static
  Group address range 232.7.7.7 to 232.7.7.9, source address 10.1.1.10
  Group address 227.7.7.7
  Group address range 227.7.7.7 to 227.7.7.9
  Group address 232.7.7.7, source address 10.1.1.10
  Interfaces using the classmap:
    Ethernet3/1
```

The following is sample output from the **show ip igmp static-group** command with the **interface** keyword. The output is self-explanatory.

```
Router# show ip igmp static-group class-map interface

Loopback0
  Class-map attached: static1
Ethernet3/1
  Class-map attached: static
```

The following is sample output from the **show ip igmp static-group** command with the **interface** keyword and *type number* arguments. The output is self-explanatory.

```
Router# show ip igmp static-group class-map interface Ethernet 3/1
Ethernet3/1
  Class-map attached: static
```

Related Commands

Command	Description
class-map type multicast-flows	Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps.
group (multicast-flows)	Defines the group entries to be associated with a IGMP static group class map.
ip igmp static-group	Configures static group membership entries on an interface.

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 10: 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 mcache

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **show ip mcache** command is not available in Cisco IOS software.

To display the contents of the IP fast-switching cache, use the **show ip mcache** command in user EXEC or privileged EXEC mode.

show ip mcache [**vrf** *vrf-name*] [*group-address*| *group-name*] [*source-address*| *source-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the contents of the IP fast-switching cache associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-address | *group-name*	(Optional) The address or name of the group for which to display the fast-switching cache. Can be either a Class D IP address or a Domain Name System (DNS) name.
source-address | *source-name*	(Optional) The specified source address or name for which to display a single multicast cache entry. Can be either a unicast IP address or a DNS name.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was 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.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Examples

The following is sample output from the **show ip mcache** privileged EXEC command when multicast distributed switching (MDS) is in effect:

```
Router# show ip mcache
IP Multicast Fast-Switching Cache
(*, 239.2.3.4), Fddi3/0/0, Last used: mds
  Tunnel3         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
  Tunnel0         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
  Tunnel1         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
```

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

Table 11: show ip mcache Field Descriptions

Field	Description
*	Source address or source wildcard (*).
239.2.3.4	Destination address.
Fddi	Incoming or expected interface on which the packet should be received.
Last used:	Latest time the entry was accessed for a packet that was successfully fast switched. The word “Semi-fast” indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process level switched.
Tunnel0 MAC Header:	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header will show the real next hop MAC header and then, in parentheses, the real interface name.

show ip mfib

To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB), use the **show ip mfib** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name*| ***}] [**all**| **linkscope**| *group-address*/*mask*| *group-address* [*source-address*]| *source-address group-address*] **[verbose]**

Syntax Description

vrf {*vrf-name* | *****	(Optional) Displays forwarding entries and interfaces in the IPv4 MFIB associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name* --Name of an MVRF. Displays forwarding entries and interfaces in the IPv4 MFIB associated with the MVRF specified for the *vrf-name* argument. • ***** --Displays a summary of traffic statistics from the IPv4 MFIB for sources and groups associated with all tables (all MVRF tables and the global table).
all	(Optional) Displays forwarding entries and interfaces in the IPv4 MFIB for both linkscope (reserved) and non-linkscope (non-reserved) groups.
linkscope	(Optional) Displays forwarding entries and interfaces in the IPv4 MFIB for linkscope (reserved) groups.
group-address / *mask*	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, which is referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.
verbose	(Optional) Includes hardware-related IPv4 MFIB flags and Cisco Express Forwarding (CEF)-related adjacency information.

Command Default If no optional keywords or arguments are entered, forwarding entries and interfaces in the IPv4 MFIB associated with nonlinkscope multicast groups are displayed.

Command Modes User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines Use the **show ip mfib** command to display IPv4 MFIB forwarding entries and interfaces.

A forwarding entry in the IPv4 MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces.

Note For a description of the significant MFIB and Multicast Routing Information Base (MRIB) forwarding entries and interface flags, see the "Multicast Forwarding Information Base Overview" module.

Examples The following is sample output from the **show ip mfib** command:

```
Router# show ip mfib 232.1.1.1
 (192.168.1.2,232.1.1.1) Flags:
   SW Forwarding: 3786/10/28/2, Other: 0/0/0
   Serial1/0 Flags: A
   Ethernet0/0 Flags: F NS
     Pkts: 3786/0
```

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

```
Router# show ip mfib
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                XO - Data Rate Above Threshold, K - Keepalive
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,224.0.0.0/4) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
 (*,224.0.1.40) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   GigabitEthernet0/0/0 Flags: F IC NS
     Pkts: 0/0
```

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

Table 12: show ip mfib Field Descriptions

Field	Description
SW Forwarding:	Statistics on the packets that are received from and forwarded out of at least one interface (packet count/packets per second/average packet size/kbits per second).
Other:	Statistics on received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Pkts	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.

show ip mfib active

To display information from the IPv4 Multicast Forwarding Information Base (MFIB) about the rate at which active multicast sources are sending to multicast groups, use the **show ip mfib active** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name*| ***}] [**all**| **linkscope**| *group-address*/*mask*| *group-address* [*source-address*]| *source-address group-address*] **active** [*kbps*]

Syntax Description

vrf {*vrf-name* | *****	(Optional) Displays the rate at which active multicast sources are sending to multicast groups associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name* --Name of an MVRF. Displays the rate at which active multicast sources are sending to multicast groups associated with the MVRF specified for the *vrf-name* argument. • ***** --Displays the rate at which active multicast sources are sending to multicast groups for all tables (all MVRF tables and the global table).
all	(Optional) Displays the rate at which active multicast sources are sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays the rate at which active multicast sources are sending to linkscope (reserved) groups.
group-address / *mask*	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, which is referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.
kbps	(Optional) Kilobits per second (kbps).

Command Default

If no optional keywords or arguments are entered, all active sources sending to nonlinkscope multicast groups at a rate greater than or less than 4 kbps are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib active** command to display active multicast streams forwarding at a rate greater than or equal to the value specified for the optional *kbps* argument. If no value is specified for the optional *kbps* argument, this command will display all active sources sending to nonlinkscope (nonreserved) multicast groups at a rate greater than or equal to 4 kbps.

Note In some cases, you may need to specify a sufficiently low value for the *kbps* argument to ensure that low data rate streams are displayed (multicast streams sending traffic at a rate less than 4 kbps).

Examples

The following sample output from the **show ip mfib active** command displays the active multicast sources that are sending traffic to nonlinkscope multicast groups at a rate greater than or equal to 1 kbps on a router participating in a multicast network.

```
Router# show ip mfib active 1
Active Multicast Sources - sending >= 1 kbps
Default
Group: 239.1.1.1
  Source: 192.168.1.2,
   SW Rate: 10 pps/2 kbps(1sec), 2 kbps(last 121 sec)
```

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

Table 13: show ip mfib active Field Descriptions

Field	Description
Active Multicast Sources - sending >=	Active multicast sources sending traffic at a rate greater than or equal to the value specified after the equal (=) sign, in kbps.
Group:	Multicast group address.
Source:	Multicast source address.
SW Rate:	Rate at which active sources are sending traffic to multicast groups.

show ip mfib count

To display summary traffic statistics from the IPv4 Multicast Forwarding Information Base (MFIB) about multicast sources and groups, use the **show ip mfib count**command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name*| *****}] [**all**| **linkscope**| *group-address*/*mask*| *group-address* [*source-address*]| *source-address group-address*] **count**

Syntax Description

vrf {*vrf-name* | *****	(Optional) Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name* --Name of an MVRF. Displays a summary of traffic statistics from the IPv4 MFIB for sources and groups associated with the MVRF specified for the *vrf-name* argument. • ***** --Displays a summary of traffic statistics from the IPv4 MFIB for sources and groups associated with all tables (all MVRF tables and the global table).
all	(Optional) Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources sending to linkscope (reserved) groups.
group-address/mask	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.

Command Default

If no optional keywords or arguments are entered, a summary of traffic statistics from the IPv4 MFIB about multicast sources sending traffic to nonreserved (nonlinkscope) multicast groups is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.

Usage Guidelines

Use the **show ip mfib count** command to display a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups, including number of packets, packets per second, average packet size, and kilobytes per second.

Examples

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

```
Router# show ip mfib count
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)
Default
 11 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 232.0.0.0/8
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 232.1.1.1
  Source: 10.1.1.1,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
  Totals - Source count: 1, Packet count: 0
Group: 232.1.1.2
  Source: 10.1.1.1,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
  Totals - Source count: 1, Packet count: 25044
Groups: 3, 0.66 average sources per group
```

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

Table 14: show ip mfib count Field Descriptions

Field	Description
Forwarding Counts	Statistics on the packets that are received and forwarded out an interface. This section tracks the following statistics: • 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. • 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. • Kilobits per second--Bytes per second divided by packets per second divided by 1000.
Other counts	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded. This section tracks the following statistics: • Total/--Total number of packets received. • RPF failed/--Number of packets not forwarded due to a failed Reverse Path Forwarding (RPF) or acceptance check (when bidirectional Protocol Independent Multicast (PIM) is configured). • Other drops(OIF-null, rate-limit etc)--Number of packets not forwarded for reasons other than an RPF failure or acceptance check (such as the outgoing interface [OIF] list was empty or because the packets were discarded because of a configuration that was enabled).

Field	Description
Default	Summary information about all the routes and groups in the MFIB database. This section tracks the following statistics: • routes--Total number of routes in the MFIB database. • (*,G)s--Total number of (*, G) entries in the MFIB database. • (*,G/m)s--Total number of groups that have a specific mask in the MFIB database.
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 Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
RP-tree:	Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*, G) groups are bidirectional PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM SSM range groups.
SW Forwarding:	Statistics on the packets that are received from and forwarded to at least one interface.
Other:	Statistics on received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Totals -	This section tracks the following statistics: • Source count--Total number of multicast sources sending to multicast groups in the IPv4 MFIB. • Packet count--Total number of packets received and forwarded. This count is cumulative for all sources in the source count.
Groups	The total number of unique groups in the MFIB database, and the average number of sources per group.

show ip mfib interface

To display IPv4 Multicast Forwarding Information Base (MFIB)-related information about interfaces and their forwarding status, use the **show ip mfib interface**command in user EXEC or privileged EXEC mode.

show ip mfib interface [**control**| **data**] [*type number*]

Syntax Description

control	(Optional) Displays interfaces in the IPv4 MFIB, and any associated control information.
data	(Optional) Displays IPv4 MFIB forwarding information about interfaces.
type number	(Optional) Interface type and number.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Examples

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

```
Router# show ip mfib interface
IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: MFIB Init Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 202
    Tables 1/1/0 (active/mrib/io)
MFIB interface             status    CEF-based output
                                   [configured,available]
GigabitEthernet0/0/0       up      [yes       ,yes      ]
GigabitEthernet0/0/1       down    [yes       ,no       ]
GigabitEthernet0/0/2       down    [yes       ,no       ]
GigabitEthernet0/0/3       down    [yes       ,no       ]
GigabitEthernet0/1/0       up      [yes       ,yes      ]
GigabitEthernet0/1/1       down    [yes       ,no       ]
GigabitEthernet0/1/2       down    [yes       ,no       ]
GigabitEthernet0/1/3       down    [yes       ,no       ]
Serial2/0                  down    [yes       ,no       ]
Serial2/1                  down    [yes       ,no       ]
Serial2/2                  down    [yes       ,no       ]
Serial2/3                  down    [yes       ,no       ]
Serial3/0                  down    [yes       ,no       ]
Serial3/1                  down    [yes       ,no       ]
```

```
Serial3/2                 down    [yes       ,no       ]
Serial3/3                 down    [yes       ,no       ]
Loopback0                 up      [yes       ,yes      ]
Tunnel0                   up      [yes       ,yes      ]
```

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

Table 15: show ip mfib interface Field Descriptions

Field	Description
IPv4 Multicast Forwarding (MFIB) status:	Displays the status of interfaces in the IPv4 MFIB.
Configuration Status	IPv4 MFIB configuration status on the interface.
Initialization State	Initialization state of the IPv4 MFIB.
MFIB interface	Lists available interfaces for which to display IPv4 MFIB status.
status	Status of the interface.
CEF-based output	Provides information about the status of Cisco Express Forwarding on the MFIB interface. This section tracks whether Cisco Express Forwarding has been configured and whether it is available on the interface.

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

```
Router# show ip mfib interface control

                                          MFIB Forwarding
MFIB interface                    IP   PIM     Process        CEF
                                            (Conf/Oper)  (Conf/Oper)
GigabitEthernet0/0/0              up   on      yes  yes     yes  yes
GigabitEthernet0/1/0              off  off     yes  no      yes  no
GigabitEthernet0/2/0              off  off     yes  no      yes  no
GigabitEthernet0/3/0              off  off     yes  no      yes  no
GigabitEthernet1/0/0              up   on      yes  yes     yes  yes
GigabitEthernet1/1/0              off  off     yes  no      yes  no
GigabitEthernet1/2/0              off  off     yes  no      yes  no
GigabitEthernet1/3/0              off  off     yes  no      yes  no
Serial2/0                         off  off     yes  no      yes  no
Serial2/1                         off  off     yes  no      yes  no
Serial2/2                         off  off     yes  no      yes  no
Serial2/3                         off  off     yes  no      yes  no
Serial3/0                         off  off     yes  no      yes  no
Serial3/1                         off  off     yes  no      yes  no
Serial3/2                         off  off     yes  no      yes  no
Serial3/3                         off  off     yes  no      yes  no
Loopback0                         up   on      yes  yes     yes  yes
Tunnel0                           up   reg     yes  out     yes  out
```

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

Table 16: show ip mfib interface control Field Descriptions

Field	Description
MFIB interface	Lists available interfaces for which to display IPv4 MFIB status.
IP	Displays the status of IP on the available interfaces.
PIM	Displays the status of PIM on the available interfaces.
Process	Displays the configuration and operational status of the IPv4 MFIB on the available interfaces.
CEF	Displays the configuration and operational status of CEF on the available interfaces.

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

```
Router# show ip mfib interface data
                                                MFIB Forwarding
MFIB interface                          Type    Process         CEF
                                                             (Active/Available)
GigabitEthernet0/0/0                    None    yes          yes    yes
GigabitEthernet1/0/0                    None    yes          yes    yes
 Loopback0                              None    yes          yes    yes
 Tunnel0                                None    out          out    out
```

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

Table 17: show ip mfib interface data Field Descriptions

Field	Description
MFIB interface	Lists available interfaces for which to display IPv4 MFIB forwarding status.
Type	Next hop type value (for example, IPv4, IPv6, LSM, LSM NBMA, MDTv4, MDTv6, None, v4Dec, and v6Dec).
Process	Displays the status of the IPv4 MFIB process.
CEF	Displays the status of Cisco Express Forwarding (whether it is active and available) for IPv4 MFIB interfaces.

show ip mfib route

To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) without packet header information and forwarding counters, use the **show ip mfib route**command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name*| ***}] **route** [**all**| **linkscope**| *group-address*/*mask*| *group-address* [*source-address*]| *source-address group-address*] [**detail**| **internal**]

Syntax Description

vrf {*vrf-name* | ***}	(Optional) Displays the forwarding entries and interfaces in the IPv4 MFIB associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name* --Name of an MVRF. Displays the forwarding entries and interfaces in the IPv4 MFIB associated with the MVRF specified for the *vrf-name* argument. • ***** --Displays the forwarding entries and interfaces in the IPv4 MFIB associated with all tables (all MVRF tables and the global table).
all	(Optional) Displays the forwarding entries and interfaces in the IPv4 MFIB for both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays the forwarding entries and interfaces in the IPv4 MFIB for linkscope (reserved) groups.
group-address / *mask*	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation (referred to as a (*, G/mask) entry).
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.
detail	(Optional) For use by Cisco technical support. Displays detailed information about the routes in the IPv4 MFIB.
internal	(Optional) For use by Cisco technical support. Displays the internal data structures for the routes in the IPv4 MFIB.

Command Default

If no optional keywords or arguments are entered, forwarding entries and interfaces in the IPv4 MFIB associated with nonlinkscope multicast groups are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib route** command to display the forwarding entries and interfaces in the IPv4 MFIB. Unlike the **show ip mfib** command, the output from this command does not display packet header information and IPv4 MFIB packet and forwarding counters.

Note For a description of the significant MFIB and Multicast Routing Information Base (MRIB) forwarding entries and interface flags, see the "Multicast Forwarding Information Base (MFIB) Overview" module.

Examples

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

```
Router# show ip mfib route
Default
 (*,224.0.0.0/4) C
 (*,224.0.1.39) C
   Loopback0 NS
   GigabitEthernet1/0/0 F NS
   GigabitEthernet0/0/0 NS
 (192.168.6.6,224.0.1.39)
   GigabitEthernet1/0/0 A NS
 (*,224.0.1.40) C
   Loopback0 F IC NS
   GigabitEthernet1/0/0 F NS
 (192.168.6.6,224.0.1.40)
   Loopback0 F IC NS
   GigabitEthernet1/0/0 A
 (*,232.0.0.0/8)
 (*,239.1.1.1) C
   GigabitEthernet1/0/0 A
 (192.168.1.2,239.1.1.1)
   GigabitEthernet1/0/0 F NS
   GigabitEthernet0/0/0 A
```

Related Commands

Command	Description
show ip mfib	Displays the forwarding entries and interfaces in the IPv4 MFIB.

show ip mfib status

To display the general IPv4 Multicast Forwarding Information Base (MFIB) configuration and operational status, use the **show ip mfib status**command in user EXEC or privileged EXEC mode.

show ip mfib status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib status** command to find such information as whether the IPv4 MFIB is enabled and running.

Examples

The following is sample output from the **show ip mfib status** command:

```
Router# show ip mfib status
IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: MFIB Init Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 202
    Tables 1/1/0 (active/mrib/io)
```

show ip mfib summary

To display summary information about the number of IPv4 Multicast Forwarding Information Base (MFIB) entries (including linkscope groups) and interfaces, use the **show ip mfib summary**command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name*| ***}] **summary** [**detail**| **internal**]

Syntax Description

vrf {*vrf-name* | ***}	(Optional) Displays summary information about the number of IPv4 MFIB entries and interfaces associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name* --Name of an MVRF. Displays summary information about the number of IPv4 MFIB entries and interfaces associated with the MVRF specified for the *vrf-name* argument. • ***** --Displays summary information about the number of IPv4 MFIB entries and interfaces associated with all tables (all MVRF tables and the global table).
detail	(Optional) For use by Cisco technical support. Displays more detailed information about the IPv4 MFIB entries and interfaces in the summary of the IPv4 MFIB.
internal	(Optional) For use by Cisco technical support. Displays internal data structures associated with IPv4 MFIB entries and interfaces in the summary of the IPv4 MFIB.

Command Default

If no optional keywords or arguments are entered, this command displays summary information about the number of IPv4 MFIB entries and interfaces from the global table.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Release	Modification
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **show ip mfib summary** command shows the IPv4 multicast routing table in abbreviated form. The command displays only the number of IPv4 MFIB entries, the number of (*, G), (S, G), and (*, G/m) entries, and the number of IPv4 MFIB interfaces.

The **show ip mfib summary** command counts all entries, including linkscope entries.

Examples

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

```
Router# show ip mfib summary
Default
 15 prefixes (15/0/0 fwd/non-fwd/deleted)
 28 ioitems (28/0/0 fwd/non-fwd/deleted)
 Forwarding prefixes: [3 (S,G), 9 (*,G), 3 (*,G/m)]
 Table id 0x0, instance 0x4B23B54
 Database: epoch 0
```

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

Table 18: show ip mfib summary Field Descriptions

Field	Description
15 prefixes (15/0/0 fwd/non-fwd/deleted)	Number of prefixes in the IPv4 MFIB and a summary of the status of the prefixes (forwarded/nonforwarded/deleted), including linkscope prefixes.
28 ioitems (28/0/0 fwd/non-fwd/deleted)	Number of interfaces in the IPv4 MFIB.
Forwarding prefixes: [3 (S,G), 9 (*,G), 3 (*,G/m)]	Total number of (S, G), (*, G), and (*, G/m) prefixes in the IPv4 MFIB.

show ip mpacket

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **show ip mpacket** is not available in Cisco IOS software.

To display the contents of the circular cache-header buffer, use the **show ip mpacket**command in privileged EXEC mode.

show ip mpacket [**vrf** *vrf-name*] [*group-address*| *group-name*] [*source-address*| *source-name*] **[quality] [detail] [read-only]**

Syntax Description

vrf *vrf-name*	(Optional) Displays the contents of the circular cache-header buffer associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-address *group-name*	(Optional) The specified group address or group name for which matching cache headers are displayed.
source-address *source-name*	(Optional) The specified source address or source name for which matching cache headers are displayed.
quality	(Optional) Displays Real-Time Transport Protocol (RTP) data quality.
detail	(Optional) Displays summary information and displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the User Datagram Protocol [UDP] port numbers).
read-only	(Optional) Specifies that the circular buffer will not be cleared of the IP multicast packet headers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.

Release	Modification
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **quality** and **read-only** keywords were added.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

This command is applicable only when the **ip multicast cache-headers** command is in effect.

Each time this command is entered, a new buffer is allocated. The summary display (when the **detail** keyword is omitted) shows the IP packet identifier, time-to-live (TTL) value, source and destination IP addresses, and a local time stamp when the packet was received.

All the arguments and keywords can be used in the same command in any combination.

Examples

The following is sample output from the **show ip mpacket** command for the group named smallgroup:

```
Router# show ip mpacket smallgroup
IP Multicast Header Cache - entry count:6, next index: 7
Key: id/ttl timestamp (name) source group
D782/117 206416.908 (company1.example.com) 192.168.228.10 224.5.6.7
7302/113 206417.908 (example.edu) 172.16.2.17 224.5.6.7
6CB2/114 206417.412 (company2.example.com) 172.16.19.40 224.5.6.7
D782/117 206417.868 (company1.example.com) 192.168.228.10 224.5.6.7
E2E9/123 206418.488 (example.com) 239.1.8.10 224.5.6.7
1CA7/127 206418.544 (company4.example.com) 192.168.6.10 224.5.6.7
```

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

Table 19: show ip mpacket Field Descriptions

Field	Description
entry count	Number of packets cached (one packet for each line in the display). The cache has lines numbered from 0 to 1024.

Field	Description
next index	The index for the next element in the cache.
id	Identification number of the IP packet.
ttl	Current TTL of the packet.
timestamp	Time-stamp sequence number of the packet.
(name)	Domain Name System (DNS) name of the source sending to the group. Name appears in parentheses.
source	IP address of the source sending to the group.
group	Multicast group address to which the packet is sent. In this example, the group address is the group name smallgroup.

Related Commands

Command	Description
ip multicast cache-headers	Allocates a circular buffer to store IP multicast packet headers that the router receives.

show ip mr proxy

To list the Reverse Path Forwarding (RPF) vector proxies received on a multicast router discovered by the Cisco IOS software, use the **show ip mr proxy**command in user EXEC or privileged EXEC mode.

show ip mr[*group*]**proxy**

Syntax Description

group	(Optional) Multicast routing group.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to determine if an RPF vector proxy is received on a core router.

Examples

The following is sample output from the **show ip mr proxy command**:

```
Router# show ip mr proxy
Proxy Table
Proxy        Assigner      Origin   Uptime/Expire
10.0.0.1     10.0.2.2      PIM      00:02:16/00:02:14
```

The table below describes the fields shown in the display.

Table 20: show ip mr proxy Field Descriptions

Field	Description
Proxy	Proxy value.
Assigner	IP address of the router assigning the proxy vector.
Origin	Protocol origin.

Field	Description
Uptime/Expires	Uptime shows how long (in hours:minutes:seconds) the entry has been in the table. Expires shows how long (in hours:minutes:seconds or in milliseconds) until the entry will be removed from the IP multicast routing table.

Related Commands

Command	Description
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Displays information about PIM neighbors.

show ip mrib client

To display information about the clients of the IPv4 Multicast Routing Information Base (MRIB), use the **show ip mrib client** command in user EXEC or privileged EXEC mode.

show ip mrib [**vrf** *vrf-name*] **client [filter]** [**name** *client-name* [: *connection-id*]]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about clients of the IPv4 MRIB associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
filter	(Optional) Displays information about the IPv4 MRIB flags each client owns and the flags each client is interested in.
name *client-name*	(Optional) Displays the name an IPv4 MRIB client. **Note** The names of the MRIB clients that can be specified for the *client-name* argument can be found by entering the **show ip mrib client** command with no optional keywords or arguments.
: *connection-id*	(Optional) The connection ID associated with the IPv4 MRIB client. The colon is required. **Note** The connection ID is typically the Process ID (PID) value associated with the MRIB client.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show ip mrib client** command to display information about the clients of the IPv4 MRIB. When this command is entered with the optional **filter** keyword, the output will display additional information, including the IPv4 MRIB flags each clients owns and the flags each client is interested in.

Note For a description of the significant MFIB and MRIB forwarding entries and interface flags, see the "Multicast Forwarding Information Base (MFIB) Overview" module.

Examples

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

```
Router# show ip mrib client
IP MRIB client-connections
MRIB Trans for MVRF #0     table:199    (connection id 1)
IPv4_mfib(0x5474934):7.196       (connection id 2)
```

The following is sample output from the **show ip mrib client** command with the **filter** and **name** keywords and *client-name* and **:** *connection-id* arguments:

```
Router# show ip mrib client filter name IPv4_mfib(0x5474934):7.196
IP MRIB client-connections
IPv4_mfib(0x5474934):7.196      (connection id 2)
  interest filter:
    entry attributes:  S C IA K ET DDE
    interface attributes:  A DP F IC NS SP
    groups:
      include 0.0.0.0/0
    interfaces:
      include All
  ownership filter:
    groups:
      include 0.0.0.0/0
    interfaces:
      include All
```

show ip mrib route

To display the routes in the IPv4 Multicast Routing Information Base (MRIB) table, use the **show ip mrib route**command in user EXEC or privileged EXEC mode.

show ip mrib [**vrf** *vrf-name*] **route** [**reserved**| [*source-address*| ***] [*group-address* [/*mask*]]]

Syntax Description

vrf *vrf-name*	(Optional) Displays routes in the IPv4 MRIB associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
reserved	(Optional) Displays routes in the IPv4 MRIB associated with linkscope groups.
source-address	(Optional) Multicast source address.
*	(Optional) Displays shared tree entries in the IPv4 MRIB.
group-address	(Optional) Multicast group address.
group-address / *mask*	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, which is referred to as a (*, G/mask) entry.

Command Default

If this command is entered without the optional **reserved** keyword, the output displays only routes in the IPv4 MRIB associated with nonreserved (nonlinkscope) groups.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show ip mrib route c**ommand to display the IPv4 MRIB table. All entries are created by various clients of the IPv4 MRIB, such as, Protocol Independent Multicast (PIM) and the IPv4 MFIB. The flags on each entry or interface act as a communication mechanism between the various clients of the IPv4 MRIB.

Note For a description of the significant MFIB and MRIB forwarding entries and interface flags, see the " Multicast Forwarding Information Base (MFIB) Overview " module.

Examples

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

```
Router# show ip mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
    ET - Data Rate Exceeds Threshold,K - Keepalive,DDE - Data Driven Event
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, MD - mCAC Denied

(*,224.0.0.0/4) Flags: C

(*,224.0.1.39) RPF nbr: 0.0.0.0 Flags: C
  Ethernet1/0 Flags: F NS
  Ethernet0/0 Flags: NS
  Loopback0 Flags: NS

(*,224.0.1.40) RPF nbr: 0.0.0.0 Flags: C
  Ethernet1/0 Flags: F NS
  Loopback0 Flags: F IC NS

(*,232.0.0.0/8) Flags:

(192.168.6.6,224.0.1.39) RPF nbr: 192.168.123.2 Flags:
  Ethernet1/0 Flags: A NS

(192.168.6.6,224.0.1.40) RPF nbr: 192.168.123.2 Flags:
  Ethernet1/0 Flags: A
  Loopback0 Flags: F IC NS
```

show ip mrib route summary

To display the total number of routes and interfaces in the IPv4 Multicast Routing Information Base (MRIB), use the **show ip mrib route summary**command in user EXEC or privileged EXEC mode.

show ip mrib [**vrf** *vrf-name*] **route summary**

Syntax Description

vrf *vrf-name*	(Optional) Displays the total number of routes and interfaces in the IPv4 MRIB associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show ip mrib summary** command to display the total number of routes and interfaces in the IPv4 Multicast Routing Information Base (MRIB).

Note The total number of routes and interfaces displayed in the output includes routes and interfaces associated with both reserved (linkscope) and nonreserved multicast groups.

Examples

The following is sample out from the **show ip mrib summary** command:

```
Router# show ip mrib summary
MRIB Route-DB Summary
  No. of (*,G) routes = 11
  No. of (S,G) routes = 2
  No. of Route x Interfaces (RxI) = 25
```

show ip mrm interface

To display Multicast Routing Monitor (MRM) information related to interfaces, use the **show ip mrm interface**command in user EXEC or privileged EXEC mode.

show ip mrm interface [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which to display MRM interface information.

Command Default

If no interface is specified for the *type* and *number* arguments, information about all interfaces participating in MRM is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display which interfaces are participating in MRM, in which roles, and whether the interfaces are up or down.

Examples

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

```
Router# show ip mrm interface
Interface           Address          Mode                 Status
Ethernet0           10.0.0.1         Test-Sender          Up
Ethernet1           10.0.0.10        Test-Receiver        Up
```

The table below describes the fields shown in the display.

Table 21: show ip mrm interface Field Descriptions

Field	Description
Interface	List of interfaces on this router that serve as a Test Sender or Test Receiver.
Address	IP address of the interface.
Mode	Role that the interface plays in MRM, either Test Sender or Test Receiver.
Status	Status of the interface.

Related Commands

Command	Description
ip mrm	Configures an interface to operate as a Test Sender or Test Receiver, or both, for MRM.

show ip mrm manager

To display information about a Multicast Routing Monitor (MRM) test, use the **show ip mrm manager**command in user EXEC or privileged EXEC mode.

show ip mrm manager [*test-name*]

Syntax Description

test-name	(Optional) Name of the MRM test for which to display information.

Command Default

If no test name is specified for the *test-name* argument, information about all Managers is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display status information and the parameters configured for an MRM test.

Examples

The following is sample output from the **show ip mrm manager** command executed at two different times:

```
Router# show ip mrm manager test
Manager:test/10.0.0.0 is running, expire:1d00h
  Beacon interval/holdtime/ttl:60/86400/32
  Group:239.1.2.3, UDP port test-packet/status-report:16384/65535
  Test senders:
    10.0.0.1 /Ack
  Test receivers:
    10.0.0.2 /Ack
Router# show ip mrm manager test
Manager:test/10.0.0.0 is not running
  Beacon interval/holdtime/ttl:60/86400/32
  Group:239.1.2.3, UDP port test-packet/status-report:16384/65535
  Test senders:
    10.0.0.1
```

```
Test receivers:
  10.0.0.2
```

The table below describes the fields shown in the display.

Table 22: show ip mrm manager Field Descriptions

Field	Description
Manager	Status of the test.
Beacon interval/holdtime/ttl	The interval at which beacon messages are sent (Beacon interval), the duration of the test period (holdtime), and the time-to-live value of beacon messages. **Note** Beacon parameters are controlled with the **beacon** command. By default, beacon messages are sent at an interval of 60 seconds; the duration of the test period is 86400 seconds (1 day); and the time-to-live of beacon messages is 32 hops.
Group	IP multicast group that the Test Receiver will listen to, as configured by the **manager** command.
UDP port test-packet/status-report	User Datagram Protocol (UDP) port number to which test packets are sent by a Test Sender and status reports are sent by a Test Receiver. **Note** The UDP port numbers to which test packets are sent by a Test Sender and status reports are sent by a Test Receiver are controlled with the **udp-port**command. By default, the Test Sender uses UDP port number 16834 to send test packets, and the Test Receiver uses UDP port number 65535 to send status reports.
Test senders	IP address of Test Senders.
Test receivers	IP address of Test Receivers.

Related Commands

Command	Description
beacon	Changes the frequency, duration, or scope of beacon messages that the Manager sends to the Test Sender and Test Receiver.
ip mrm manager	Specifies the name of an MRM test to be created or modified, and enters MRM manager configuration mode.

Command	Description
manager	Specifies that an interface is the Manager for MRM, and specifies the multicast group address the Test Receiver will listen to.
udp-port	Changes the UDP port numbers to which the Test Sender sends test packets or the Test Receiver sends status reports.

show ip mrm status-report

To display the status reports in the Multicast Routing Monitor (MRM) status report cache, use the **show ip mrm status-report**command in user EXEC or privileged EXEC mode.

show ip mrm status-report [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of a Test Receiver for which to display status reports.

Command Default

If no IP address is specified for the optional *ip-address* argument, all status reports in the MRM status report cache are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show ip mrm status-report** command during your MRM test period to learn if any errors are reported. The Manager immediately displays error reports and sends error reports, if any, to the circular status report cache. The cache holds up to 1024 lines, with one line for each error report.

No errors reported indicates that the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

Use the **show ip mrm status-report** command with the optional *ip-address* argument to restrict the output to display only status reports sent by the Test Receiver at the specified IP address. If no IP address is specified for the optional *ip-address* argument, all status reports in the MRM status report cache are displayed.

Use the **clear ip mrm status-report** command to clear the MRM status report cache.

Examples

The following is sample output from the **show ip mrm status-report** command:

```
Router# show ip mrm status-report
IP MRM status report cache:
Timestamp        Manager         Test Receiver   Pkt Loss/Dup (%)      Ehsr
*Apr 20 07:36:08 10.0.0.0        10.0.0.1        5            (20%)    0
*Apr 20 07:36:09 10.0.0.0        10.0.0.1        10           (40%)    0
*Apr 20 07:36:10 10.0.0.0        10.0.0.1        15           (60%)    0
```

The table below describes the fields shown in the display.

Table 23: show ip mrm status-report Field Descriptions

Field	Description
Timestamp	Time when the status report arrived in the cache. Month and date, hours:minutes:seconds.
Manager	IP address of the Manager.
Test Receiver	IP address of the Test Receiver.
Pkt Loss/Dup	Number of packets lost or duplicated.
(%)	Percentage of packets lost or duplicated. Loss percentage is calculated based on the **packet-delay**value of the **senders** command, which defaults to 200 milliseconds (or 5 packets per second). If the default for the **window** keyword (5 seconds) is not changed, then the Test Receiver expects 5 packets per second for 5 seconds = 25 packets. If the Test Receiver receives only 15 packets, then 25 - 15 = 10 lost packets. Lost packets divided by packets expected equals loss percentage; 10/25 equals a loss percentage of 40 percent. A negative percentage indicates duplicate packets were received. If the packet loss reaches 100 percent, the Test Receiver will not send periodic reports until the packet loss decreases to less than 100 percent.
Ehsr	Extended highest sequence number received from Real-Time Transport Protocol (RTP).

Related Commands

Command	Description
clear ip mrm status-report	Clears the MRM status report cache.

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 24: 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 25: 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 26: 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 27: 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 rpf-peer

To display the unique Multicast Source Discovery Protocol (MSDP) peer information from which a router will accept Source-Active (SA) messages originating from the specified rendezvous point (RP), use the **show ip msdp rpf-peer**command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **rpf-peer** *rp-address*

Syntax Description

vrf *vrf-name*	(Optional) Displays MSDP information about a peer from which the router will accept SA messages that originated from an RP associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rp-address	Address of the rendezvous point (RP).

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command when you need MSDP information about a peer from which the router will accept SA messages that originated from an RP. The **ip msdp rfc-3618 rpf-rules** command must be configured for the **show ip msdp rpf-peer**command to generate output.

Examples

The following is sample output for the **show ip msdp rpf-peer**command:

```
Router# show ip msdp rpf-peer 10.0.0.0
RPF peer information for ? (25.8.8.8)
RPF peer: ? (2.2.2.3)
RPF route/mask: 0.0.0.0/0
RPF rule: Peer is IGP next hop of best route
RPF type: unicast (rip)
```

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

Table 28: show ip msdp rpf Field Descriptions

Field	Description
RPF peer information for	Reverse Path Forwarding (RPF) peer address for the specified RP address. The question mark (?) indicates that the system does not find a name for that particular address.
RPF peer:	Peer address from which this device would accept MSDP SAs originated by the specified RP address. The question mark (?) indicates that the system does not find a name for that particular address.
RPF route/mask:	Network and mask of the RP address that the system determines from the route lookups that it used to choose the RPF peer.
RPF rule:	Rule used to determine the RPF peer for the specified RP address.
RPF type:	Route lookup or protocol used to choose the RPF peer for the specified RP address.

Related Commands

Command	Description
ip msdp rpf rfc3618	Enables IETF RFC 3618-compliant MSDP peer-RPF forwarding rules.

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 29: 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 30: 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 31: 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 multicast

To display information about IP multicast global configuration parameters, use the **show ip multicast**command in user EXEC or privileged EXEC mode.

show ip multicast {[**vrf** *vrf-name*]| **vif**}

Syntax Description

vrf *vrf-name*	(Optional) Restricts the output to displaying IP multicast global configuration parameters associated with the Multicast VPN Routing and Forwarding (MVRF) instance specified by the *vrf-name* argument.
vif	(Optional) Restricts the output to displaying configuration parameters associated with the Labeled Switched path (LSP) for the multicast virtual host interface (VIF) in the global table.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)ZW	This command was integrated into Cisco IOS Release 12.2(33)ZW.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.3(1)S	This command was modified. The **vif** keyword was added.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release XE 3.8S.

Examples

The following is sample output from the **show ip multicast** command. The output is self-explanatory.

```
Router# show ip multicast
  Multicast Routing: enabled
  Multicast Multipath: disabled
  Multicast Route limit: No limit
  Limit for number of sources per group: 10
  Limit for number of OIFs in this MVRF: 8000
```

```
  The pim is turned off in this MVRF as the configured
    OIFs limit per MVRF has reached.
  Limit for number of OIFs in the router: 8000
  Multicast Triggered RPF check: enabled
  Multicast Fallback group mode: Dense
```

The table below describes the fields shown in the display.

Table 32: show ip multicast Field Descriptions

Field	Description
Multicast Routing	Indicates whether multicast routing has been enabled or disabled (using the **ip multicast-routing** command).
Multicast Multipath	Indicates whether multicast load splitting has been enabled or disabled (using the **ip multicast multipath** command) and displays what hash algorithm is configured for load splitting IP multicast traffic (when multicast load splitting has been enabled).
Multicast Route limit	Displays the limit configured for the **ip multicast route-limit** command.
Limit for number of sources per group	Displays the limit configured for the number of sources in a group.
Limit for number of OIFs in this MVRF	Displays the limit configured for the number of outgoing interfaces (OIFs) in the MVRF.
The pim is turned off in this MVRF as the configured OIFs limit per MVRF has reached	Indicates that Protocol Independent Multicast (PIM) is turned off for the MVRF as the configured OIFs limit per MVRF has been reached.
Limit for number of OIFs in the router	Displays the configured limit for the total number of OIFs in the router.
Multicast Triggered RPF check	Indicates whether RPF triggered RPF checks have been enabled (the default) or disabled (using the **no ip multicast rpf backoff**command)
Multicast Fallback group mode	Indicates the multicast fallback group mode (dense or sparse) in use (configured with the **ip pim dm-fallback** command). The default is dense mode.

Related Commands

Command	Description
ip multicast multipath	Enables load splitting of IP multicast traffic over ECMP.

Command	Description
ip multicast oif-per-mvrf-limit	Configures the limit for number of OIFs per default MVRF.
ip multicast-routing	Enables IP multicast routing.
ip multicast multipath	Enables load splitting of IP multicast traffic over ECMP.
ip multicast route-limit	Limits the number of mroutes that can be added to a multicast routing table.
ip multicast rpf backoff	Configures the intervals at which PIM RPF failover will be triggered by changes in the routing tables.
ip multicast source-per-group-limit	Configures the limit for the total number of sources for a group per default MVRF.
ip multicast total-oif-limit	Configures the limit for the total number of OIFs in a router.
ip pim dm-fallback	Enables PIM-DM fallback.

show ip multicast interface

To display information about IP multicast interface configuration parameters and packet counters, use the **show ip multicast interface**command in user EXEC or privileged EXEC mode.

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

Syntax Description

vrf *vrf-name*	(Optional) Restricts the output to displaying information about multicast-enabled interfaces associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified by the *vrf-name* argument.
type number	(Optional) Interface type and number for which to display IP multicast interface-specific configuration paratemeters and packets counters.

Command Default

If no optional arguments and keywords are specified, this command will display IP multicast configuration parameters and packet counters for all multicast-enabled interfaces.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)ZW	This command was integrated into Cisco IOS Release 12.2(33)ZW.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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.

Examples

The following is sample output from the **show ip multicast interface** command with *type number* arguments:

```
Router# show ip multicast interface fastethernet 1/0
FastEthernet1/0 is up, line protocol is up
  Internet address is 10.1.1.1/24
  Multicast routing: enabled
  Multicast switching: fast
  Multicast packets in/out: 0/0
  Multicast boundary: test       (in/out)
```

```
  Multicast Tagswitching: disabled
  Multicast TTL threshold: 0
  Multicast Tagswitching: disabled
```

The table below describes the fields shown in the display.

Table 33: show ip multicast interface Field Descriptions

Field	Description
<interface type> <interface number> is	Indicates the state of the multicast-enabled interface (up or down).
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
IP address is	IP address configured for the interface (using the ip address command)
Multicast routing:	Indicates whether multicast routing (Protocol Independent Multicast [PIM]) has been enabled or disabled on the interface (using the **ip pim** command).
Multicast switching:	Indicates the type of multicast switching operating on the interface (as configured with the **ip mroute-cache**command). **Note** In Cisco IOS Releases that support the IPv4 MFIB, the **ip mroute-cache** command has been removed and this field will always display “fast” in the output.
Multicast packets in/out:	Displays multicast packet counters. **Note** These counters are also displayed in the output of the **show ip pim interface** command.
Multicast boundary:	Indicates the multicast boundary configured on an interface (using the **ip multicast boundary** command). **Note** If no IP multicast boundaries are configured on the interface, this field will not be displayed in the output.
Multicast TTL threshold:	Indicates the time-to-live (TTL) threshold of multicast packets being forwarded out an interface (as configured with the **ip multicast ttl-threshold** command). **Note** This field is obsolete in Cisco IOS Releases that support the IPv4 MFIB. For those releases, the **ip multicast ttl-threshold** command has been removed and this field will always “0” in the output.

Field	Description
Multicast Tagswitching:	This field is obsolete. It will always display “Disabled” in the output.

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip mroute-cache	Configures IP multicast fast or distributed switching on interface.
ip multicast boundary	Configures an administratively scoped IPv4 multicast boundary on an interface.
ip multicast ttl-threshold	Configures the TTL threshold of multicast packets being forwarded out an interface.
show ip pim interface	Displays information about interfaces configured for PIM.

show ip multicast redundancy state

To display information about the current redundancy state for IP multicast, use the **show ip multicast redundancy state** command in user EXEC or privileged EXEC mode.

Syntax for the Catalyst 6500 Series Switch in Cisco IOS Release 12.2(33)SXI and Later Releases

show ip multicast redundancy state

Syntax for the Cisco 7600 Series Router in Cisco IOS Release 12.2(33)SRE, Cisco IOS Release 15.0(1)S, and Later Releases

show ip multicast redundancy state [verbose]

Syntax Description

verbose	(Optional) Displays additional information about the In Service Software Upgrade (ISSU) negotiation status for each defined IP multicast synchronization message type.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was modified. The **verbose** keyword was added, and new output fields were added to display ISSU status information.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use this command to display the current IP multicast redundancy state of the Route Processors (RPs). The output displays information about the current multicast redundancy state of the RPs and the current synchronization state of the standby RP.

Examples

The following is sample output from the **show ip multicast redundancy state** command from a Catalyst 6500 series switch running Cisco IOS Release 12.2(33)SXI:

```
Router# show ip multicast redundancy state
Multicast Redundancy state:   SSO
Sync message epoch:           0
Sync message sequence number: 11
```

```
Stale NSF state flush timeout: 30000 ms
Current sync state: Synched
```

The table below describes the fields shown in the display.

Table 34: show ip multicast redundancy state Field Descriptions

Field	Description
Multicast Redundancy state:	Indicates the current redundancy state of the RPs.
Sync message epoch:	Internal qualifier for the synchronization message sequence number.
Sync message sequence number:	Internal sequence number assigned to a synchronization message within a synchronization message epoch.
Stale NSF state flush timeout:	Indicates the nonstop forwarding (NSF) state flush timeout period. **Note** In the event of an RP switchover, this timeout period occurs after unicast and multicast reconvergence. The timeout period is the delay between the downloading of refreshed multicast control plane route information to the forwarding plane and the flushing of stale NSF forwarding plane information that was retained from before the RP switchover. The default timeout period is 30,000 milliseconds (ms). Use the **ip multicast redundancy routeflush maxtime** command to configure an additional timeout period before stale forwarding plane multicast routing (mroute) information is flushed.
Current sync state:	Current synchronization state of the standby RP.

The following is sample output from the **show ip multicast redundancy state** command from a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRE:

```
Router# show ip multicast redundancy state
Multicast IPv4 Redundancy Mode:   SSO
Multicast IPv6 Redundancy Mode:   Not enabled
Multicast IPv4 HA state machine status: Idle
Multicast IPv6 HA state machine status: Idle
Sync message epoch:           0
Sync message sequence number: 21
Stale NSF state flush timeout: 30000 ms
Current sync state: Synched
Multicast ISSU Client Status:
  PIM MIC client            ISSU compatible
  MRIB MIC client           ISSU compatible
  MFIB IPv4 MIC client      ISSU compatible
  MFIB IPv6 MIC client      No ISSU result reported
  PLATFORM IPv4 MIC client  Unregistered - ignored
  PLATFORM IPv6 MIC client  Unregistered - ignored
```

```
  IPv4 SSO supported for:   PIM, MRIB, MFIBV4
  IPv6 SSO blocked by:      MFIBV6
```

The following is sample output from the **show ip multicast redundancy state** command with the **verbose** keyword from a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRE:

```
Router# show ip multicast redundancy state verbose
Multicast IPv4 Redundancy Mode:   SSO
Multicast IPv6 Redundancy Mode:   Not enabled
Multicast IPv4 HA state machine status: Idle
Multicast IPv6 HA state machine status: Idle
Sync message epoch:           0
Sync message sequence number: 21
Stale NSF state flush timeout: 30000 ms
Current sync state: Synched
Multicast ISSU Client Status:
  PIM MIC client            ISSU compatible
  MRIB MIC client           ISSU compatible
  MFIB IPv4 MIC client      ISSU compatible
  MFIB IPv6 MIC client      No ISSU result reported
  PLATFORM IPv4 MIC client  Unregistered - ignored
  PLATFORM IPv6 MIC client  Unregistered - ignored
  IPv4 SSO supported for:   PIM, MRIB, MFIBV4
  IPv6 SSO blocked by:      MFIBV6
Multicast ISSU sync message status
SYNC_RP_MAPPING               : Compatible
SYNC_RP_ROUTE                 : Compatible
SYNC_BSR                      : Compatible
SYNC_AUTORP_DISCOV_IDB        : Compatible
SYNC_MDB                      : Compatible
SYNC_MIDB                     : Compatible
SYNC_MSDP                     : Compatible
SYNC_RPDF                     : Compatible
SYNC_MDT_TUNNEL               : Compatible
SYNC_REG_TUNNEL               : Compatible
SYNC_MCAC_RSV                 : Compatible
SYNC_MDT_DATA_RCV             : Compatible
SYNC_MDT_DATA_SND             : Compatible
SYNC_MDT_DATA_RCV_DECAP       : Compatible
SYNC_LSP_VIF                  : Compatible
```

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

Table 35: show ip multicast redundancy state Field Descriptions

Field	Description
Multicast IPv4 Redundancy Mode:	Indicates the current redundancy mode in operation for IPv4 multicast.
Multicast IPv6 Redundancy Mode:	Indicates the current redundancy mode in operation for IPv6 multicast.

Field	Description
Multicast IPv4 HA state machine status:	

Field	Description
	Provides the status of IPv4 high availability (HA) state machine events. **Note** This status is displayed only on the active RP. Possible state machine status values are as follows: • DDE replaying • Flush pending • Idle • Not enabled • NSF hold-off extending • Unicast converging Following an RP switchover, the multicast NSF HA state machine is enabled under the following conditions: • The system is configured to be in stateful switchover (SSO) mode. • All registered IPv4 multicast software components (Protocol Independent Multicast [PIM], Multicast Routing Information Base [MRIB], Multicast Forwarding Information Base [MFIB], and, on applicable router types, the platform multicast driver software) have successfully completed ISSU negotiation with their peer on the "old" active RP before the RP switchover occurred. • Multicast routing is configured for the default multicast routing table or for one or more nondefault multicast routing tables (for example, VPN routing and forwarding [VRF] instances). If the multicast IPv4 HA state machine is not enabled, the state machine status displayed is "Not enabled." If the multicast IPv4 HA state machine is enabled, the state machine status progresses through the following states after a switchover occurs: • Unicast converging--Indicates that this RP is gathering updated multicast and unicast routing information from neighboring routers and hosts for one or more IPv4 multicast routing tables. This phase of the state machine must complete before the next phase, data driven events (DDE) replay, can begin.

Field	Description
	• DDE replaying--Indicates that this RP is incorporating synched MFIB state information for multicast (S,G) routes that were created before the switchover by DDEs into the multicast routing table. This information is being incorporated for one or more IPv4 multicast routing tables. Multicast routes learned via DDEs cannot be learned from neighboring PIM routers or hosts and are, instead, synched by the MFIB during steady state operation in order to enable data flow continuity through an SSO switchover. DDEs comprise one of the two following types: • • Initial start of data flow from a directly connected data source (host) that is detected on a “first hop” router. • Shortest path tree (SPT) switchover at a “last hop” router that is triggered by multicast data packets received via a (*, G) multicast route from a given source “S” and sent to an Internet Group Management Protocol (IGMP) host that has requested reception of packets from a multicast group address “G.” • NSF hold-off extending--Indicates that after completion of DDE replay, an additional NSF hold-off delay was requested by the platform multicast driver software for one or more IPv4 multicast routing tables. The hold-off period will continue until it is either released by the platform multicast driver software or until the maximum allowable hold-off time has elapsed. This phase of the HA state machine is optional and occurs only when required for correct serialization of platform multicast driver software databases during initial postswitchover processing. • Flush pending--Indicates that the multicast HA state machine is waiting for the hold-off period to flush “stale” multicast data plane forwarding state.

Field	Description
	After the hold-time period ends (the period when the current converged multicast routing control plane state is downloaded to the multicast data plane software and hardware), a “flush” is performed to delete any multicast forwarding state that was previously stored in the data plane (through synching from the “old” active RP during steady state operation) that has not been “refreshed” by matching state from the reconverged post failover routing information in the multicast control plane. A fixed time delay is observed between the termination of the hold-off period and the flushing of stale multicast data plane forwarding state. • Idle--Indicates that the multicast HA state machine has completed its progression through all state machine phases for all IPv4 multicast routing tables. Following the flushing of stale multicast data plane state, normal multicast route and forwarding state maintenance has resumed.
Multicast IPv6 HA state machine status:	Provides the status of IPv6 HA state machine events. **Note** This status is displayed only on the active RP. The field descriptions for the IPv6 HA state machine are nearly the same as for the IPv4 HA state machine; therefore, you can apply the field descriptions from the IPv4 HA state machine, substituting IPv6 for IPv4. The one exception is that the conditions for enabling the IPv6 HA state machine are slightly different (because the Multicast VPN feature is not supported for the IPv6 address family). The conditions required for enabling the IPv6 multicast HA state machine are, therefore, as follows: • The system is configured to be in SSO mode • All registered IPv6 multicast software components (PIM, MRIB, MFIB, and, on applicable router types, the platform multicast driver software) have successfully completed ISSU negotiation with their peer on the “old” active RP before the RP switchover occurred. • Multicast routing is configured for the IPv6 multicast address family.

Field	Description
Sync message epoch:	Internal qualifier for the synchronization message sequence number.
Sync message sequence number:	Internal sequence number assigned to a synchronization message within a synchronization message epoch.
Stale NSF state flush timeout:	Indicates the NSF state flush timeout period. **Note** In the event of an RP switchover, this timeout period occurs after unicast and multicast reconvergence. The timeout period is the delay between the downloading of refreshed multicast control plane route information to the forwarding plane and the flushing of stale NSF forwarding plane information that was retained from before the RP switchover. The default timeout period is 30,000 ms. Use the **ip multicast redundancy routeflush maxtime** command to configure an additional timeout period before stale forwarding plane mroute information is flushed.
Current sync state:	Current synchronization state of the standby RP.
Multicast ISSU Client Status:	Provides status on the various ISSU clients. Multicast requires participation from multiple software components, each of which require their own communication channel to the standby RP. ISSU client status tracks ISSU negotiation state for each of these components.
Multicast ISSU sync message status:	Provides the status of ISSU synchronization messages. For each type of internal multicast forwarding database, ISSU requires agreement from the active and standby peers on which message version will be used. These outputs show that the negotiation completion status for each of the synched database types.

Related Commands

Command	Description
debug ip multicast redundancy	Displays information about IP multicast redundancy events.

Command	Description
ip multicast redundancy routeflush maxtime	Configures an additional timeout period before stale forwarding plane mroute information is flushed following an RP switchover.
show ip multicast redundancy statistics	Displays IP multicast redundancy statistics.

show ip multicast redundancy statistics

To display IP multicast redundancy statistics, use the **show ip multicast redundancy statistics** command in user EXEC or privileged EXEC mode.

show ip multicast redundancy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **show ip multicast redundancy statistics** command to display IP multicast redundancy statistics. The output displays the following information:

- A summary statistic showing the current number of synchronization messages awaiting transmission from the active Route Processor (RP) to the standby RP. (This count is summed across all synchronization database types.)
- A summary statistic showing the current number of synchronization messages that have been sent from the active RP to the standby RP, but for which the active RP has not yet received acknowledg ment from the standby for successful reception. (This count is summed across all synchronization database types.)
- The last two statistics, displaying the count of messages awaiting transmission or acknowledgement, provide a way to measure the load on the internal synchronization message sending mechanism.

Use the **clear ip multicast redundancy statistics** command to reset IP multicast redundancy statistics.

Examples

The following is sample output from the **show ip multicast redundancy statistics** command:

```
mcast-iouha-1# show ip multicast redundancy statistics
Multicast Redundancy Statistics
Sync Type              Updates       Syncs        Sync failures
RP mapping              0            0            0
Bidir. RP route info    0            0            0
Bootstrap cache         0            0            0
Autorp discovery IDB    0            0            0
RPDF                    0            0            0
```

```
MDT tunnel              0            0            0
PIM register tunnel     0            0            0
MCAC Reservation        0            0            0
Data MDT receive        0            0            0
Data MDT send           0            0            0
Data MDT receive decap  0            0            0
Lspvif                  0            0            0
Requests Awaiting Sync Msg Transmission: 0
Requests Awaiting Sync Msg Acknowledgement: 0
```

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

Table 36: show ip multicast redundancy statistics Field Descriptions

Field	Description
Sync Type	Displays statistics about the internal multicast forwarding databases that are synchronized between the active and standby RP. The following internal multicast forwarding databases are synchronized between the active and standby RPs: • RP mapping--Internal database that stores group-to-RP mapping information. • Bidirectional (bidir) RP route info--Internal database that stores bidir-Protocol Independent Multicast (PIM) RP route information. • Bootstrap cache--Internal database that stores bootstrap router (BSR) candidate information. • AutoRP discovery IDB--Internal database that stores the identity of the interface chosen on the active RP for use as the source interface for AutoRP discovery messages. • RPDF--Internal database that stores bidir-PIM designated forwarder (DF) information. • MDT tunnel--Internal database that stores MVPN Multicast Distribution Tree (MDT) tunnel information. • PIM register tunnel--Internal database that stores Protocol Independent Multicast (PIM) register tunnel information. • MCAC Reservation--Internal database that stores the identity of IPv6 (S, G) multicast routes for which a multicast Call Admission Control (MCAC) cost is currently accrued for each interface on the active RP. Retention of this information on the standby RP enables that RP, on becoming the new active RP during an RP switchover, to reserve MCAC bandwidth for these multicast routes during the initial post switchover multicast state reconvergence period, which, therefore, enables continuity of these multicast data streams through an RP switchover.

Field	Description
Updates	Tracks the number of updates that required standby RP synchronization for each of the internal multicast forwarding databases. If the number of updates displayed under the "Updates" column for an internal multicast forwarding database matches the number of synchronizations displayed under the "Syncs" column, it can be inferred that the standby RP is currently synchronized. **Note** Over time, however, the number of updates for a given multicast forwarding database is expected to exceed the number of synchronizations. In normal operating conditions, this disparity is usually due to update bundling: when several updates are sent simultaneously (or within a relatively short period of time), the Cisco IOS software will bundle the updates when synchronizing data on the standby RP. **Note** If the number of updates exceeds the number of synchronizations because of a synchronization failure, then the number displayed under "Sync failures" will also increment.
Syncs	Number of times that the data for a given internal multicast forwarding database has been synchronized on the standby RP.

Field	Description
Sync failures	Number of times that synchronization of data for a given internal multicast forwarding database failed on the standby RP. **Tip** The **show ip multicast redundancy state** command can be used to determine the synchronization state after a synchronization failure. When the standby RP has been resynchronized after a failure, the current state shown in the "Current sync state" field will display "Synched." **Note** An alternative way to determine whether the standby RP has been resynchronized is to examine the "Requests Awaiting Sync Msg Transmission" and the "Requests Awaiting Sync Msg Acknowledgement" fields. The value displayed for these fields will normally be zero (except in situations where the system is under heavy load). In the event of a synchronization failure, the number of synchronization message requests for updates awaiting transmission and acknowledgment will begin accumulating in the queue; the values displayed for those fields, thus, will increment accordingly. After the standby RP recovers from the failure and resynchronizes, the value displayed for those fields will return to zero.
Requests Awaiting Sync Msg Transmission:	Synchronization message requests that are in the queue for transmission from the active RP to the standby RP.
Requests Awaiting Sync Msg Acknowledgement:	Synchronization message requests that are in transit awaiting acknowledgment from the standby RP.

Field	Description
Average Sync Wait Time =	Displays the average time, in milliseconds (ms), that a synchronization message request for an update waits in the queue before being sent to the standby RP. **Note** Both this field and the "Average Sync Ack Time =" field can be interpreted as a measure of how heavy the load is on the synchronization message sending mechanism. The average wait time for a synchronization message request in the queue will generally be short (even on a heavily loaded system). On a lightly loaded system, the value displayed for this field may even appear as 0 ms (when the wait time is less than half of a millisecond, the system will round down to zero).
Average Sync Ack Time =	Displays the average round-trip time of synchronization message requests for updates, in milliseconds (ms). The average for the round-trip time is based on the time between when messages are sent to the standby RP for acknowledgment to the time at which the active RP receives acknowledgments from the standby RP for those messages. **Note** The average time that is displayed for this field will always be higher than the average time displayed for the "Average Sync Wait Time" field; however--even on a heavily loaded system--the average time displayed for this field will generally be short.

Related Commands

Command	Description
clear ip multicast redundancy statistics	Resets IP multicast redundancy statistics.
debug ip multicast redundancy	Displays information about IP multicast redundancy events.

show ip multicast rpf tracked

To display IP multicast Return Path Forwarding (RPF) tracked information, use the **show ip multicast rpf tracked**command in user EXEC or privileged EXEC mode.

show ip multicast rpf tracked

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Examples

The following is sample output from the **show ip multicast rpf tracked**command.

```
Router# show ip multicast rpf tracked
RPF interface: Ethernet0
  RPF neighbor: ? (10.0.10.2)
  RPF route/mask: 10.0.33.0/16
  RPF type: unicast (eigrp 1)
  RPF recursion count: 0
```

Related Commands

Command	Description
debug ip multicast rpf tracked	Displays information about IP multicast rpf tracked events.

show ip multicast topology

To display multicast topology information, use the **show ip multicast topology**command in user EXEC or privileged EXEC mode.

show ip multicast topology [{**multicast**| **unicast**} *topology-name*]

Syntax Description

multicast *topology-name*	(Optional) Displays information about the specified multicast topology instance.
unicast *topology-name*	(Optional) Displays information about the specified unicast topology instance.

Command Default

Information about all topology instances is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

This command displays topology information for multicast streams that are configured to support the Multicast Live-Live feature. This feature delivers two multicast streams with the same content over diverse paths in the network. This functionality reduces packet loss due to network failures on any one of the paths.

Examples

The following is sample output from the **show ip multicast topology**command:

```
Router# show ip multicast topology multicast live-A
Topology: ipv4 multicast live-A
TID: 1
 Extended IP ACL: 101
Associated VPN VRF is IPv4 default
```

The table below describes the fields shown in the display.

Table 37: show ip multicast topology Field Descriptions

Field	Description
Topology	The multicast data stream topology instance whose information is being displayed.
TID	The identity of the topology instance.
Extended IP ACL	The IP access list that is associated with the topology instance.
Associated VPN VRF	The Virtual Private Network (VPN) Virtual Routing and Forwarding (VRF) instance that is associated with the topology instance.

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast rpf select topology	Associates a multicast topology with a multicast group with a specific mroute entry.
ip multicast topology	Configures topology selection for multicast streams.

show ip pgm host defaults

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display the default values for Pragmatic General Multicast (PGM) Host traffic, use the **show ip pgm host defaults**command in user EXEC or privileged EXEC mode.

show ip pgm host defaults

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.1(1)T	This command was introduced.
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 default values displayed in the **show ip pgm host defaults** command output are applied to every new host connection that is opened.

Examples

The following is sample output from the **show ip pgm host defaults** user EXEC command:

```
Router> show ip pgm host defaults
Source Session Default Values :

    spm-ambient-ivl (6000), txw-adv-secs (6000)
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

Receiver Session Default Values :

    nak-gen-ivl (60000), nak-rb-ivl (500), nak-rdata-ivl (2000)
    nak-rpt-ivl (2000), rx-buffer-mgmt (minimum), rx-local-retrans (none)

Common Default Values:
```

```
    stream-type (apdu), ttl (255)
Address used to source packets:(10.1.1.1)
```

The table below describes the fields and default values in the sample output.

Table 38: show ip pgm host defaults Field Descriptions

Field	Description
Source Session Default Values	Displays the values for source-specific PGM Host traffic defaults.
spm-ambient-ivl (6000)	Amount of time, in milliseconds, the PGM Host waits for a PGM source path message (SPM) ambient data packet. The default is 6000 ms.
txw-adv-secs (6000)	Amount of time, in milliseconds, of the advanced transmit window for the PGM Host. The default is 6000 ms.
txw-adv-timeout-max (3600000)	Amount of time, in milliseconds, the PGM Host waits for data packets, even if the PGM Host receives PGM NAK data packets. The default is 3600000 ms.
txw-rte (16384)	The data transmit rate, in bytes-per-second, for the PGM Host. The default is 16384 bytes per second.
txw-secs (30000)	Data transmit window size, in milliseconds, for the PGM Host. The default is 30000 ms.
ncf-max (infinite)	Maximum number of PGM NAK confirmation data packets (NAK NCFs), in packets per second, the PGM Host sends per second. The default is infinite.
spm-rpt-ivl (3000)	Amount of time, in milliseconds, the PGM Host waits for a PGM SPM repeat data packet. The default is 3000 ms.
ihb-min (1000)	SPM interheartbeat timer minimum, in milliseconds. The default is 1000 ms.
ihb-max (10000)	SPM interheartbeat timer maximum, in milliseconds. The default is 10000 milliseconds (ms).
join (0)	Amount of time, in milliseconds, the PGM Host waits, when running in router mode, for client requests. The default is 0 ms.
tpdu-size (16384)	Size of the source transport data unit (TPDU) for the PGM Host. The available range is 41 through 16384 bytes. The default is 1400 bytes.

Field	Description
tx-adv-method (time)	Type of advanced transmit window method (data or time) for the PGM Host. The default is time.
tx-buffer-mgmt (return)	Type of transmit data buffers (keep or return) for the PGM Host. The default is return.
Receiver Session Default Values	Displays the values for receiver-specific PGM Host traffic defaults.
nak-gen-ivl (60000)	Amount of time, in milliseconds, the PGM Host waits for a PGM negative acknowledgment (NAK) data packet. The default is 60000 ms.
nak-rb-ivl (500)	Amount of time, in milliseconds, the PGM Host waits before sending a PGM NAK data packet. The default is 500 ms.
nak-rdata-ivl (2000)	Amount of time, in milliseconds, the PGM Host waits for a re-sent PGM NAK (NAK RDATA) data packet. The default is 2000 ms.
nak-rpt-ivl (2000)	Amount of time, in milliseconds, the PGM Host waits for a PGM NAK confirmation (NAK NCF) data packet. The default is 2000 ms.
rx-buffer-mgmt (minimum)	Type of receive data buffers (full or minimum) for the PGM Host. The default is minimum.
rx-local-retrans (none)	Specifies whether a receiver has to do local retransmissions or not if it sees NAKs.
Common Default Values	Displays the values for PGM Host traffic defaults that are common between a source and a receiver.
stream-type (apdu)	Data stream type (apdu or byte) for the PGM Host. The default is apdu.
ttl (255)	Time-to-live (TTL) value on the PGM Host for sent multicast data packets. The default is 255 hops. The TTL value for a packet is decremented by 1 as the packet passes through a router.
Address used to source packets	The unicast IP address that the virtual host is using to originate PGM packets.

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm host sessions	Displays open PGM Host traffic sessions.
show ip pgm host traffic	Displays PGM Host traffic statistics.

show ip pgm host sessions

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display open Pragmatic General Multicast (PGM) Host traffic sessions, use the **show ip pgm host sessions**command in user EXEC or privileged EXEC mode.

show ip pgm host sessions [*session-number*| *group-address*]

Syntax Description

session-number	(Optional) PGM Host traffic session number.
group-address	(Optional) PGM Host multicast group address.

Command Default

No default behavior or values

Command Modes

User EXEC Privileged EXEC

Command History

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

Usage Guidelines

If a session number or multicast group address is not specified, all open traffic sessions are displayed.

Examples

The following user EXEC example shows all open traffic sessions:

```
Router> show ip pgm host sessions
Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
1    000000000000  0            receiver listen  48059      224.3.3.3
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1
```

The following user EXEC example shows traffic information for traffic session number 2:

```
Router> show ip pgm host sessions 2
Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1
```

```
    stream-type (apdu), ttl (255)

    spm-ambient-ivl (6000), txw-adv-secs (6000)
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      6
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0
    General bad packets                     0
    TX window lead                          0
    TX window trail                         0
```

The following user EXEC example shows traffic information for multicast group address 244.1.1.1:

```
Router> show ip pgm host sessions 244.1.1.1
Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1

    stream-type (apdu), ttl (255)

    spm-ambient-ivl (6000), txw-adv-secs (6000)
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      6
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0
    General bad packets                     0
    TX window lead                          0
    TX window trail                         0
```

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

Table 39: show ip pgm host sessions Field Descriptions

Field	Description
Idx	The local index for the traffic session.
GSI	The global source identifier for the traffic session.
Source Port	The source port for the traffic session.
Type	Source or receiver session.

Field	Description
State	The state of the session. For example, connected or listening.
Dest Port	The destination port for the traffic session.
Mcast Address	The IP multicast address for the traffic session.
ODATA	Normal data packet.
RDATA	Re-sent data packet.
ADPUs	Application data units.
SPM	Source path message.
NCF	Negative acknowledgment (NAK) confirmation packet.
NAK	NAK packet.

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm host defaults	Displays the default values for PGM Host traffic.
show ip pgm host traffic	Displays PGM Host traffic statistics.

show ip pgm host traffic

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display Pragmatic General Multicast (PGM) Host traffic statistics, use the **show ip pgm host traffic**command in user EXEC or privileged EXEC mode.

show ip pgm host traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

User EXEC Privileged EXEC

Command History

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

Usage Guidelines

Use this command to display traffic statistics at the PGM transport layer.

Examples

The following is sample output from the **show ip pgm host traffic** user EXEC command:

```
Router> show ip pgm host traffic
General Statistics :

    Sessions in                             0
             out                            0
    Bytes    in                             0
             out                            0

Source Statistics :

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
```

```
    APDU  transmit memory errors            0
    SPM   packets sent                      0
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0

Receiver Statistics :

    ODATA packets received                  0
          packets received in error         0
          valid bytes received              0
    RDATA packets received                  0
          packets received in error         0
          valid bytes received              0
    Total valid bytes received              0
    Total bytes received in error           0
    ADPUs received                          0
    SPM   packets received                  0
          packets received in error         0
    NCF   packets received                  0
          packets received in error         0
    NAK   packets received                  0
          packets received in error         0
          packets sent                      0
    Undeliverable packets                   0
    General bad packets                     0
    Bad checksum packets                    0
```

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

Table 40: show ip pgm host traffic Field Descriptions

Field	Description
General Statistics	Displays statistics that relate to both the traffic source and the receiver.
Source Statistics	Displays statistics that relate to the traffic source.
Receiver Statistics	Displays statistics that relate to the traffic receiver.

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm host defaults	Displays the default values for PGM Host traffic.
show ip pgm host sessions	Displays open PGM Host traffic sessions.

show ip pgm router

To display Pragmatic General Multicast (PGM) Reliable Transport Protocol state and statistics, use the **show ip pgm router**command in user EXEC or privileged EXEC mode.

show ip pgm router[**interface**[*interface-type interface-number*]| **state**[*group-address*]| **traffic**[*interface-type interface-number*]][**verbose**]

Syntax Description

interface [*interface-type interface-number*]	(Optional) Displays interfaces on which PGM Router Assist is configured.
state [*group-address*	(Optional) Displays designated local repairer (DLR) information and PGM resend state information per transport session identifier (TSI). If no group address is specified, resend state for all groups is shown.
traffic [*interface-type interface-number*	(Optional) Displays PGM packet counters. If no interface type and number are specified, traffic on all interfaces is displayed. These statistics do not reflect the number of PGM data packets (ODATA) that are forwarded in a session, because these are forwarded transparently by IP multicast. **Note** The **traffic** keyword will display statistics for the POLRs, NAKs, RDATA that will differentiate if they are taken from the off-tree DLR (or the upstream DLR in some cases). POLLs have rows for POLLs received and POLLs discarded. In the case of POLLs for off-tree DLR discovery, the packets are discarded and are accounted for in the POLLs discarded row.
verbose	(Optional) Displays extended information about outgoing interface lists, timers, and Forward Error Connections (FECs).

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	The output display for this command was updated to include DLR information.

Release	Modification
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.

Examples

The following is sample output from the **show ip pgm router**command with the **interface** keyword:

```
Router# show ip pgm router interface
Address         Interface
10.1.0.2       Ethernet1/0/0 (measured drop rate 0%)
10.3.0.2       Ethernet1/0/4 (measured drop rate 0%)
```

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

Table 41: show ip pgm router Field Descriptions

Field	Description
Address	IP address of the interface running PGM Router Assist.
Interface	Interface type and number on the router that is running PGM Router Assist, plus the drop rate measured on the interface.

The following is sample output from the **show ip pgm router**command with the **traffic** keyword. An RDATA fragment is a part of an RDATA packet that has been fragmented at the IP layer while in transit. The PGM network element has seen two RDATA packets that were each fragmented into three IP fragments.

```
Router# show ip pgm router traffic
FastEthernet0/0
  NAKs received                 2
  NCFs transmitted              2
 RDATA forwarded                2
 RDATA frags forwarded          6
  SPMs received                 4
       used                     4
  SPMs forwarded               33
Serial0/0
  NAKs forwarded                2
  NAKs retransmitted            2
  NCFs received                 4
 RDATA received                 2
 RDATA frags received           6
  SPMs received                33
       used                    33
```

The following is sample output from the **show ip pgm router**command with the **state** and **verbose** keywords. The timer associated with each session is an idle timer; the TSI state is deleted when this timer expires. The measured loss rates are indicated as follows:

- link_lr: worst reported link loss rate

- path_lr: worst reported path loss rate
- receiver_lr: worst reported receiver loss rate
- cr_lead: sequence number associated with worst receiver loss rate
- cr_worst_rec: IP address that reported worst loss rate

```
Router# show ip pgm router state verbose
TSI                 Group            Neighbor        TGSIZE
0A0700C85555-1000  227.7.7.7        rpf/source       N/A        00:04:25
  (link_lr 7%, path_lr 4%, receiver_lr 10%
  cr_lead 6256421, cr_worst_rec 134.45.0.126)
```

The following sample output shows state after receivers have reported loss of certain packets. Negative acknowledgments (NAKs) have been received for each of the two sessions in the previous example. After the loss, the router has state for the lost packets. The “sqn 1990” indicates that a receiver lost a packet with sequence number 1990 and is requesting that it be re-sent.

```
Router# show ip pgm router state verbose
TSI                 Group            Neighbor        TGSIZE
0A0700C85555-1000  227.7.7.7        rpf/source       N/A        00:04:55
   sqn        1990            age   4 ELIM TMR
       Ethernet1/0/0
   sqn        1991            age    5 (anticipated)
0A0700C85555-2000 234.4.3.2         rpf/source       16         00:04:55
   sqn (       125,          7) age   10
       Serial5/0 prty # 7
```

For the selective TSI, the output shows resend state for sequence number 1990. This state was created by a NAK received on Ethernet interface 1/0/0. “ELIM TMR” indicates that the state is eliminating duplicates of any NAK that is pending and any new NAKs for this sequence number will not be forwarded.

State shown for sequence 1991 is anticipated state, indicating that it was created by a NAK confirmation (NCF) for a NAK sent by some other PGM router with the same PGM upstream neighbor as this router.

For the TSI with parity, the state shown was created by a parity NAK for seven packets of the Transmission Group 125. This state was received on serial interface 5/0; “# 7” indicates that seven parity packets must be forwarded out this interface.

Related Commands

Command	Description
clear ip pgm router	Clears PGM traffic statistics.
ip pgm router	Enables PGM Router Assist and thereby allows PGM to operate more efficiently on the router.

show ip pim boundary

To display information about mroutes filtered by administratively scoped IPv4 multicast boundaries configured on an interface, use the **show ip pim boundary** command in user EXEC or privileged EXEC mode.

show ip pim boundary *interface-type interface-number* **source-address group-address** {**in**| **out**}

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
source- address	IP address or hostname of the source.
group- address	IP address or hostname of the group.
in	Displays whether an mroute is being filtered (blocked) by an incoming multicast boundary (a multicast boundary configured to filter source traffic coming into the interface).
out	Displays whether an mroute is being filtered (blocked) by an outgoing multicast boundary (a multicast boundary configured to prevent mroutes states from being created on an interface by filtering Protocol Independent Multicast (PIM) joins and Internet Group Management Protocol (IGMP) reports for groups or channels).

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(1)	This command was introduced in a release earlier than Cisco IOS Release 12.4(1).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the the **show ip pim boundary** command to determine whether an mroute is being filtered by administratively scoped IPv4 multicast boundaries configured on an interface (using the **ip multicast boundary** command).

Examples

The following sample output from the **show ip pim boundary** command shows a blocked mroute entry. The field descriptions are self-explanatory.

```
Router# show ip pim boundary FastEthernet 0/0 10.1.1.1 239.159.1.1 in
(10.1.1.1,239.159.1.1) unblocked on FastEthernet0/0 for in option
```

The following sample output from the **show ip pim boundary** command shows an unblocked mroute entry. The field descriptions are self-explanatory.

```
Router# show ip pim boundary FastEthernet 1/1 10.1.1.2 239.159.1.2 out
(10.1.1.2,239.159.1.2) blocked on FastEthernet1/1 for out option
```

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped IPv4 multicast boundary.

show ip pim bsr-router

To display information about a bootstrap router (BSR), use the **show ip pim bsr-router**command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **bsr-router**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about a BSR associated with the multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

User EXEC Privileged EXEC

Command History

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

Usage Guidelines

The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Examples

The following is sample output from the **show ip pim bsr-router** command:

```
Router# show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds
Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

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

Table 42: show ip pim bsr-router Field Descriptions

Field	Description
BSR address	IP address of the BSR.
Uptime	Length of time that this router has been up (in hours, minutes, and seconds).
BSR Priority	Priority as configured with the **ip pim bsr-candidate** command.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured with the **ip pim bsr-candidate** command.
Next bootstrap message in	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Cand_RP_advertisement in	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.
RP	List of RP IP addresses.
Group acl	Standard IP access list number that defines the group prefixes that are advertised in association with the RP address. This value is configured with the **ip pim rp-candidate** command.

Related Commands

Command	Description
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.
show ip pim rp-hash	Displays which RP is being selected for a specified group.

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.
15.3(2)S	This command was modified. The output has been modified to include information about interfaces configured for BFD support for multicast (PIM).
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

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 sample output from the **show ip pim interface** command indicates that Ethernet interface 0/0 is enabled for BFD support for multicast (PIM):

```
7.2.2 show ip pim interface
Address          Interface           Ver/  Nbr      Query  DR     DR          BFD
                                     Mode  Count    Intvl  Prior
40.10.2.2        Ethernet0/0         v2/S   1        30    1      40.10.2.2   on
40.11.2.1        Ethernet0/2         v2/S   1        30    1      40.11.2.2   off
```

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 43: 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.

Field	Description
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.
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 44: show ip pim interface detail Field Descriptions

Field	Description
Internet address	IP address of the specified interface.

Field	Description
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.
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 45: 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 mdt bgp

To show details about the Border Gateway Protocol (BGP) advertisement of the route distinguisher (RD) for the multicast distribution tree (MDT) default group, use the show ip pim mdt bgp command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **mdt bgp**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about the BGP advertisement of the RD for the MDT default group associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to show detailed BGP advertisement of the RD for the MDT default group.

Examples

The following is sample output from the **show ip pim mdt bgp**command:

```
Router# show ip pim mdt bgp
MDT-default group 232.2.1.4
 rid:10.1.1.1 next_hop:10.1.1.1
```

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

Table 46: show ip pim mdt bgp Field Descriptions

Field	Description
MDT-default group	The MDT default groups that have been advertised to this router.
rid:10.1.1.1	The BGP router ID of the advertising router.
next_hop:10.1.1.1	The BGP next hop address that was contained in the advertisement.

show ip pim mdt history

To display information about the history of data multicast distribution tree (MDT) groups that have been reused, use the **show ip pim mdt history**command in privileged EXEC mode.

show ip pim vrf *vrf-name* **mdt history interval** *minutes*

Syntax Description

vrf *vrf-name*	Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interval *minutes*	Specifies the interval (in minutes) for which to display information about the history of data MDT groups that have been reused. The range is from 1 to 71512 minutes (7 weeks).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output of the **show ip pim mdt history** command displays the history of reused MDT data groups for the interval specified with the **interval** keyword and *minutes* argument. The interval is from the past to the present, that is, from the time specified for the *minutes* argument to the time at which the command is issued.

Examples

The following is sample output from the **show ip pim mdt history**command:

```
Router# show ip pim vrf vrf1 mdt history interval 20
   MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group        Number of reuse
```

```
10.9.9.8          3
10.9.9.9          2
```

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

Table 47: show ip pim mdt history Field Descriptions

Field	Description
MDT-data group	The MDT data group for which information is being shown.
Number of reuse	The number of data MDTs that have been reused in this group.

show ip pim mdt receive

To display the data multicast distribution tree (MDT) group mappings received from other provider edge (PE) routers, use the **show ip pim mdt receive**command in privileged EXEC mode.

show ip pim vrf *vrf-name* **mdt receive [detail]**

Syntax Description

vrf *vrf-name*	Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
detail	(Optional) Provides a detailed description of the data MDT advertisements received.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.11)SY.

Usage Guidelines

When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then it will join this global address multicast group.

Examples

The following is sample output from the **show ip pim mdt receive**command using the **detail** keyword for further information:

```
Router# show ip pim vrf vpn8 mdt receive detail
Joined MDT-data groups for VRF:vpn8
group:172.16.8.0 source:10.0.0.100 ref_count:13
```

```
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

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

Table 48: show ip pim mdt receive Field Descriptions

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of (S, G) pairs that are reusing this data MDT.
OIF count:1	Number of interfaces out of which this multicast data is being forwarded.
flags:	Information about the entry. • A--candidate Multicast Source Discovery Protocol (MSDP) advertisement • B--bidirectional group • D--dense • C--connected • F--register flag • I--received source-specific host report • J--join shortest path source tree (SPT) • L--local • M--MSDP created entry • P--pruned • R--RP bit set • S--sparse • s--Source Specific Multicast (SSM) group • T--SPT bit set • X--proxy join timer running • U--URL Rendezvous Directory (URD) • Y--joined MDT data group • y--sending to MDT data group • Z--multicast tunnel

show ip pim mdt send

To display the data multicast distribution tree (MDT) groups in use, use the **show ip pim mdt send** command in privileged EXEC mode.

show ip pim vrf *vrf-name* **mdt send**

Syntax Description

vrf *vrf-name*	Displays the data MDT groups in use by the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
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 Releaes 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command to show the data MDT groups in use by a specified MVRF.

Examples

The following is sample output from the **show ip pim mdt send** command:

```
Router# show ip pim vrf vpn8 mdt send
MDT-data send list for VRF:vpn8
  (source, group)                      MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)             232.2.8.0           1
  (10.100.8.10, 225.1.8.2)             232.2.8.1           1
  (10.100.8.10, 225.1.8.3)             232.2.8.2           1
  (10.100.8.10, 225.1.8.4)             232.2.8.3           1
  (10.100.8.10, 225.1.8.5)             232.2.8.4           1
  (10.100.8.10, 225.1.8.6)             232.2.8.5           1
  (10.100.8.10, 225.1.8.7)             232.2.8.6           1
  (10.100.8.10, 225.1.8.8)             232.2.8.7           1
```

```
  (10.100.8.10, 225.1.8.9)            232.2.8.8           1
  (10.100.8.10, 225.1.8.10)           232.2.8.9           1
```

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

Table 49: show ip pim mdt send Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of (S, G) pairs that are reusing this data MDT.

show ip pim neighbor

To display information about Protocol Independent Multicast (PIM) neighbors discovered by PIMv1 router query messages or PIMv2 hello messages, use the **show ip pim neighbor** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **neighbor** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about PIM neighbors associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.

Command Default

Information about all PIM neighbors is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was modified. The command output was updated to display the PIM protocol version.
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	Support for this command was introduced on the Supervisor Engine 720.
12.0(30)S	This command was modified. The “P” flag was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was modified. The “P” flag was added.

Release	Modification
12.2(31)SB2	This command was modified. The “P” flag was added.
12.2(33)SXH	This command was modified. The “P” flag was added.
12.4(20)T	This command was modified. The “P” flag was added.
12.2(33)SXI	This command was modified. The “G” flag was added.
12.2(33)SRE	This command was modified. The “G” flag was added.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use this command to display PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages.

Use the optional *interface-type* and *interface-number* arguments to restrict the output to display only information about the PIM neighbor reachable on the specified interface.

Examples

The following is sample output from the **show ip pim neighbor** command:

```
Router# show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      S - State Refresh Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.0.0.1          GigabitEthernet10/2      00:01:29/00:01:15 v2    1 / S
10.0.0.3          GigabitEthernet10/3      00:01:15/00:01:28 v2    1 / DR S P
```

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

Table 50: show ip pim neighbor Field Descriptions

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	The total uptime of the neighbor (in hours:minutes:seconds).
Expires	The time before a neighbor is timed out and until the next PIM hello is received (in hours:minutes:seconds).
Ver	The version of PIM running on the neighbor’s interface.

Field	Description
DR Prio	The priority of the PIM interface for designated router (DR) election. The possible values that can be displayed under this column are as follows: a value from 0 to 4294967294 or the "N" flag. The default DR priority is set to 1. **Note** The DR priority can be modified using the **ip pim dr-priority** command in interface configuration mode. When a DR is a candidate for election, the following conditions apply: • The router with the highest priority value configured on an interface will be elected as the DR. If this priority value is the same on multiple routers, then the router with the highest IP address configured on an interface will be elected as the DR. • If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers with this priority status, then the router with the highest IP address configured on an interface will be elected as the DR.
	Note For interoperability, if a PIM neighbor is running a release prior to Cisco IOS Release 12.1(2)T, which does not support the DR priority feature, the "DR Prio" column displays the "N" flag. If the neighbor is the only router displaying the "N" flag for a PIM interface, it becomes the DR regardless of which router actually has the highest IP address. If there are several PIM neighbors with the "N" flag listed under this column, the tiebreaker is the highest IP address among them.

Field	Description
Mode	Information about the DR and other PIM capabilities: • B--Indicates that the PIM neighbor is bidirectional PIM (bidir-PIM) capable. In a bidir-PIM network, this capability is necessary for the routers to successfully perform the designated forwarder election process. If a router detects through PIM hello messages that one of its PIM neighbors is not bidir-PIM capable, the designated forwarder election process is aborted and forwarding of bidir-PIM traffic to and from that interface would stop. • DR--Indicates that the PIM neighbor is acting as the DR. • G--Indicates that the PIM neighbor supports Generation ID (GenID) capabilities, which enable fast PIM multicast route (mroute) reconvergence times after a switchover. • P--Indicates that the neighbor has announced through PIM hello messages its capability to handle Reverse Path Forwarding (RPF) vectors in PIM join messages. All Cisco IOS versions that support the PIM RPF Vector feature announce this PIM hello option. An RPF vector is included in PIM messages only when all PIM neighbors on a RPF interface support it. • S--Indicates that the PIM neighbor supports PIM-DM state refresh capabilities (applies only to PIM neighbors running in dense mode). This flag was introduced in support of the PIM Dense Mode State Refresh feature. PIM-DM state refresh capabilities protect pruned state in PIM dense mode from timing out by periodically forwarding a control message down the source-based distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the distribution tree. By default, all PIM routers that are operating in dense mode (and are running a Cisco IOS software release that supports the PIM Dense Mode State Refresh feature) automatically process and forward state refresh control messages.

Related Commands

Command	Description
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 the PIM dense mode state refresh control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.

show ip pim 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 51: 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 pim rp mapping

To display the mappings for the PIM group to the active rendezvous points, use the **show ip pim rp mapping**command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp mapping** [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
rp-address	(Optional) Rendezvous-point IP address.

Command Default

If you do not specify an *rp-address*, the mappings for all the active rendezvous points are displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to add the **vrf***vrf-name* keyword and argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The output was modified to add the values for auto-RP and BSR mapping count and limit.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

In Cisco IOS Release 15.2(1)S and later releases, the output includes the values for auto-RP or BSR mapping count and limit:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 192.168.255.101 (?), v2v1
    Info source: 192.168.255.101 (?), elected via Auto-RP
         Uptime: 00:01:38, expires: 00:02:52
Auto-RP mapping count 1, limit 2
```

This example shows how to display the mappings for the PIM group to the active rendezvous points:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP-mapping agent
Group(s) 172.16.0.0/16
RP 10.6.6.6 (?), v2v1
Info source: 10.6.6.6 (?), elected via Auto-RP ---> learned via Auto-RP
and the elected RP.
Uptime: 22:36:49, expires: 00:02:04
Group(s) 192.168.0.0/24
RP 10.9.9.9 (?), v2v1, bidir
Info source: 10.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:20, expires: 00:02:37
Group(s) 172.16.0.0/24
RP 10.2.2.2 (?), v2v1, bidir
Info source: 10.2.2.2 (?), elected via Auto-RP
Uptime: 22:36:24, expires: 00:02:29
Group(s) 172.16.0.0/24
RP 10.9.9.9 (?), v2v1, bidir
Info source: 10.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:21, expires: 00:02:35
```

The table below describes the fields that are shown in the example.

Table 52: show ip pim rp mapping Field Descriptions

Field	Description
Info source	ACL number.
Static	Group-to-mapping information from the static rendezvous-point configuration.
Bidir Mode	Status of whether the rendezvous point is operating in bidirectional mode.
RP	Address of the rendezvous point for that group.
(?)	Status that shows no Domain Name System (DNS) name has been specified.
count	Number of RP or BSR groups configured.
limit	Maximum number of PIM groups that can be created.

Related Commands

Command	Description
ip pim maximum group-mappings	Configures PIM group mapping ranges.

show ip pim rp-hash

To display which rendezvous point (RP) is being selected for a specified group, use the **show ip pim rp-hash**command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp-hash** {*group-address*| *group-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	RP information for the specified group address or name as defined in the Domain Name System (DNS) hosts table.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(23)S	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.
12.2(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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays which RP was selected for the group specified. It also shows whether this RP was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Examples

The following is sample output from the **show ip pim rp-hash** command with the group address 239.1.1.1 specified:

```
Router# show ip pim rp-hash 239.1.1.1
RP 172.16.24.12 (mt1-47a.cisco.com), v2
    Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
         Uptime: 05:15:33, expires: 00:02:01
```

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

Table 53: show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the RP for the group specified (239.1.1.1). Within parentheses is the DNS name of the RP. If the address of the RP is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	Indicates from which system the router learned this RP information, along with the DNS name of the source. RP was selected by the bootstrap mechanism. In this case, the BSR is also the RP.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this RP.
expires	Time (in hours, minutes, and seconds) after which the information about this RP expires. If the router does not receive any refresh messages in this time, it will discard information about this RP.

show ip pim rp-hash (BSR)

To display which rendezvous point is being selected for a specified group, use the **show ip pim rp-hash**command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp-hash** {*group-address*| *group-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
group-address | *group-name*	Rendezvous-point information for the specified group address or name as defined in the DNS hosts table.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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 rendezvous point was selected for the group specified. It also shows whether this rendezvous point was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Examples

This example shows how to display which rendezvous point is being selected for a specified group:

```
Router# show ip pim rp-hash 239.1.1.1
RP 172.16.24.12 (mt1-47a.cisco.com), v2
    Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
         Uptime: 05:15:33, expires: 00:02:01
```

The table below describes the fields shown in the display.

Table 54: show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the rendezvous point for the group specified (239.1.1.1). The DNS name of the rendezvous point within the parentheses. If the address of the rendezvous point is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 is configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	Which system the router learned this rendezvous-point information and the DNS name of the source. The rendezvous point was selected by the bootstrap mechanism. In this case, the BSR is also the rendezvous point.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this rendezvous point.
expires	Time (in hours, minutes, and seconds) after which the information about this rendezvous point expires. If the router does not receive any refresh messages in this time, it discards information about this rendezvous point.

show ip pim snooping

To display the information about IP PIM snooping, use the **show ip pim snooping**command in user EXEC or privileged EXEC mode.

Global Status

show ip pim snooping

VLAN Status

show ip pim snooping vlan *vlan-id* [**neighbor| mac-group| statistics**| **mroute** [*source-ip*| *group-ip*]]

Syntax Description

vlan *vlan-id*	Displays information for a specific VLAN; valid values are from 1 to 4094.
neighbor	(Optional) Displays information about the neighbor database.
mac-group	(Optional) Displays information about the GDA database in Layer 2.
statistics	(Optional) Displays information about the VLAN statistics.
mroute	(Optional) Displays information about the mroute database.
source-ip	(Optional) Source IP address.
group-ip	(Optional) Group IP address.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	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 is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the information about the global status:

```
Router# show ip pim snooping
Global runtime mode: Enabled
Global admin mode  : Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 10
```

This example shows how to display the information about a specific VLAN:

```
Router# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
```

This example shows how to display the information about the neighbor database for a specific VLAN:

```
Router# show ip pim snooping vlan 10 neighbor
IP Address       Mac address     Port Uptime/Expires    Flags
10.10.10.2       000a.f330.344a  3/13 00:09:57/00:01:22
10.10.10.1       000a.f330.334a  3/12 00:09:44/00:01:21
10.10.10.4       000a.f330.3c00 15/01 00:09:57/00:01:22 DR
Number of Neighbors = 3
```

This example shows how to display the information about the GDA database for a specific VLAN in Layer 2:

```
Router# show ip pim snooping vlan 10 mac-group

Mac address    Group address    Uptime/Expires       Outgoing Ports
VLAN 10: 4 mac entries
0100.5e03.0101 225.3.1.1        4d01h/00:03:04       1/2 1/3 1/48 15/1
0100.5e02.0101 225.2.1.1        4d01h/00:03:13       1/2 1/3 1/48 15/1
0100.5e05.0101 225.5.1.1        4d01h/00:03:01       1/2 1/3 1/48 15/1
0100.5e04.0101 225.4.1.1        4d01h/00:03:19       1/2 1/3 1/48 15/1
PE.100#
PE.100#
PE.100#
PE.100#
```

This example shows how to display the detailed statistics for a specific VLAN:

```
Router# show ip pim snooping vlan 10 statistics
PIMv2 statistics for vlan 10:
Hello                                          : 811
Join/Prunes                                    : 1332
RP DF Election                                 : 0
Asserts                                        : 133
Other types                                    : 0
Hello option holdtime [1]                      : 811
Hello option Generation ID[20]                 : 544
Hello option DR priority[19]                   : 544
Hello option Bi-dir capable[22]                : 0
Hello option Fast Hold[65005]                  : 0
Hello option Lan Prune Delay[2]                : 0
Hello option Tag switching [17]                : 0
Hello option PIM-DM State Refresh[21]          : 544
Hello option Deprecated Cisco DR priority[18]  : 0
Error - Hello length too short                 : 0
Error - Hello hold option missing              : 0
Error - Hello option length                    : 0
Error - Hello option unknown                   : 0
Error - Join/Prune Address Family              : 0
```

```
Error - Join/Prune Parser malloc failure        : 0
Error - Join/Prune Unknown up/down neighbor     : 0
Error - Join/Prune Malformed packet discards    : 0
Error - RPDF election Address Family            : 0
Error - RPDF Unknown up/down neighbor           : 0
Error - Generic packet input error              : 0
```

This example shows how to display the information about the mroute database for all mrouters in a specific VLAN:

```
Router# show ip pim snooping vlan 10 mroute
Number of Mroutes = 6
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
VLAN 10: 4 mroutes
(*, 225.3.1.1), 4d01h/00:03:06
  10.10.10.120->10.10.10.105, 4d01h/00:03:06 , J
  Downstream ports: 1/2
  Upstream ports: 1/48
  Outgoing ports: 1/2 1/48
(*, 225.2.1.1), 4d01h/00:03:11
  10.10.10.130->10.10.10.120, 4d01h/00:03:11 , J
  Downstream ports: 1/3
  Upstream ports: 1/2
  Outgoing ports: 1/2 1/3
(*, 225.5.1.1), 4d01h/00:02:57 10.10.10.120->
  10.10.10.10, 4d01h/00:02:49 , J
  10.10.10.130->10.10.10.10, 4d01h/00:02:57 , J
  10.10.10.105->10.10.10.10, 4d01h/00:02:41 , J
  Downstream ports: 1/2 1/3 1/48
  Upstream ports: 15/1
  Outgoing ports: 1/2 1/3 1/48 15/1
(*, 225.4.1.1), 4d01h/00:03:16
  10.10.10.105->10.10.10.130, 4d01h/00:03:16 , J
  Downstream ports: 1/48
  Upstream ports: 1/3
  Outgoing ports: 1/3 1/48
```

This example shows how to display the information about the PIM mroute for a specific source address:

```
Router# show ip pim snooping vlan 10 mroute 172.16.100.100
(*, 172.16.100.100), 00:16:36/00:02:36
  10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
```

This example shows how to display the information about the PIM mroute for a specific source and group address:

```
Router# show ip pim snooping vlan 10 mroute 192.168.0.0 172.16.10.10
(192.168.0.0, 172.16.10.10), 00:03:04/00:00:25
  10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
```

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

Table 55: show ip pim snooping Field Descriptions

Field	Description
Downstream ports	Ports on which PIM joins were received.
Upstream ports	Ports towards RP and source.

Field	Description
Outgoing ports	List of all upstream and downstream ports for the multicast flow.

Related Commands

Command	Description
ip pim snooping (global configuration)	Enables PIM snooping globally.
ip pim snooping (interface configuration)	Enables PIM snooping on an interface.

show ip pim tunnel

To display information about Protocol Independent Multicast (PIM) tunnel interfaces, use the **show ip pim tunnel**command in user EXEC or privileged EXEC mode.

show ip pim [**all-vrfs**| **vrf** *vrf-name*] **tunnel** [*interface-number*] **[verbose]**

Syntax Description

all-vrfs	(Optional) Displays information about PIM tunnel interfaces associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances (including the global table).
vrf *vrf-name*	(Optional) Displays information about PIM tunnel interfaces associated with the MVRF instances associated with MVRF specified for the *vrf-name* argument.
interface-number	(Optional) PIM tunnel interface number.
verbose	(Optional) Displays detailed information about PIM tunnel interfaces.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **show ip pim tunnel**command to display information about PIM tunnel interfaces.

PIM tunnel interfaces are used by the IPv4 Multicast Forwarding Information Base (MFIB) for the PIM sparse mode (PIM-SM) registration process. Two types of PIM tunnel interfaces are used by the the IPv4 MFIB:

- A PIM encapsulation tunnel (PIM Encap Tunnel)
- A PIM decapsulation tunnel (PIM Decap Tunnel).

The PIM Encap Tunnel is dynamically created whenever a group-to-Rendezvous Point (RP) mapping is learned (via Auto-RP, bootstrap router (BSR), or static RP configuration). The PIM Encap Tunnel is used to encapsulate multicast packets sent by first-hop Designated Routers (DRs) that have directly connected sources.

Similar to the PIM Encap Tunnel, the PIM Decap Tunnel interface is dynamically created--with the exception that it is created only on the RP whenever a group-to-RP mapping is learned. The PIM Decap Tunnel interface is used by the RP to decapsulate PIM register messages.

Note PIM tunnels will not appear in the running configuration.

The following syslog message will appear when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>, changed state
to up
```

Examples

The following is sample output from the **show ip pim tunnel** command taken from a RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP.

```
Router# show ip pim tunnel
Tunnel0
  Type  : PIM Encap
  RP    : 192.168.6.6*
  Source: 192.168.6.6
Tunnel1
  Type  : PIM Decap
  RP    : 192.168.6.6*
  Source: -
```

Note The asterisk (*) indicates that the router is the RP. The RP will always have a PIM Encap and Decap Tunnel interface.

The following is sample output from the **show ip pim tunnel** command taken from a non-RP. The output is used to confirm that a PIM Encap Tunnel has been created on a non-RP router.

```
Router# show ip pim tunnel
Tunnel0
  Type  : PIM Encap
  RP    : 192.168.6.6
  Source: 192.168.67.7
```

show ip pim vc

To display ATM virtual circuit (VC) status information for multipoint VCs opened by Protocol Independent Multicast (PIM), use the **show ip pim vc**command in user EXEC or privileged EXEC mode.

show ip pim vc [*group-address*| *group-name*] [*interface-type interface-number*]

Syntax Description

group-address | *group-name*	(Optional) IP multicast group or name. Displays only the single group.
interface-type interface-number	(Optional) Interface type and number. Displays only the single ATM interface.

Command Default

VC status information is displayed for all ATM interfaces.

Command Modes

User EXEC Privileged EXEC

Command History

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

Examples

The following is sample output from the **show ip pim vc** command:

```
Router# show ip pim vc
IP Multicast ATM VC Status
ATM0/0 VC count is 5, max is 200
Group            VCD   Interface    Leaf Count  Rate
224.2.2.2        26    ATM0/0       1           0 pps
224.1.1.1        28    ATM0/0       1           0 pps
224.4.4.4        32    ATM0/0       2           0 pps
224.5.5.5        35    ATM0/0       1           0 pps
```

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

Table 56: show ip pim vc Field Descriptions

Field	Description
ATM0/0	ATM slot and port number on the interface.
VC count	Number of VCs opened by PIM.
max	Maximum number of VCs that PIM is allowed to open, as configured by the **ip pim vc-count** command.
Group	IP address of the multicast group to which the router is multicasting.
VCD	Virtual circuit descriptor.
Interface	Outgoing interface.
Leaf Count	Number of routers that have joined the group and are members of that multipoint VC.
Rate	Rate (in packets per second) as configured by the **ip pim minimum-vc-rate** command.

Related Commands

Command	Description
ip pim multipoint-signalling	Enables PIM to open ATM multipoint switched VCs for each multicast group that a receiver joins.

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 57: 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 58: 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 59: 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 ip rpf select

To display group-to-VPN routing and forwarding (VRF) mappings, use the **show ip rpf select** command in user EXEC or privileged EXEC mode.

show ip rpf [**vrf** *vrf-name*] **select**

Syntax Description

vrf *vrf-name*	(Optional) Displays the multicast group-to-VRF mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Default

If the optional **vrf** keyword and *vrf-name* argument are omitted, the **show ip rpf select** command displays all group-to-VRF mappings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip rpf select** command after configuring group-based VRF selection policies to display the configured group-to-VRF mappings. The output displays information about group-based VRF selection policies, including the group address, the VRF mapped to the group where the Reverse Path Forwarding (RPF) lookup is performed, and the name of the access control list (ACL) applied to the policy.

Use the **ip multicast rpf select** command to configure group-based VRF selection policies. By defining group-based VRF selection policies, you can configure RPF lookups originating in a receiver MVRF or in the global routing table to be resolved in a source MVRF or in the global routing table based on group address.

Examples

The following is sample output from the **show ip rpf select** command:

```
Router# show ip rpf select
Multicast Group-to-Vrf Mappings
Group(s): 227.7.1.1/32, RPF vrf: blue, Acl: 20
Group(s): 227.7.7.7/32, RPF vrf: blue, Acl: 20
Group(s): 239.1.1.1/32, RPF vrf: blue, Acl: 20
```

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

Table 60: show ip rpf select Field Descriptions

Field	Description
Group(s)	Multicast group address that is being mapped.
RPF vrf	VRF where the RPF lookup for the multicast group is performed.
Acl	ACL that the multicast group matched.

Related Commands

Command	Description
ip multicast rpf select	Configures RPF lookups based on group address.

show ip sap

To display the Session Announcement Protocol (SAP) cache, use the **show ip sap**command in user EXEC or privileged EXEC mode.

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

Syntax Description

group-address	(Optional) The sessions defining the specified multicast group address.
" *session-name* "	(Optional) Displays the single session in detail format. The session name is enclosed in quotation marks (" ") that the user must enter.
detail	(Optional) Displays all sessions in detail format.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.1	The **show ip sdr** command was introduced.
12.2	The **show ip sdr**command was replaced by the **show ip sap**command.
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

If the router is configured to be a member of multicast group 224.2.127.254 (the default session directory group), it will cache SAP announcements.

If no arguments or keywords are used with this command, the system displays a sorted list of session names.

Examples

The following is sample output from the **show ip sap** command for a session using multicast group 224.2.197.250:

```
Router# show ip sap 224.2.197.250
SAP Cache - 198 entries
Session Name: Session1
   Description: This broadcast is brought to you courtesy of Name1.
   Group: 0.0.0.0, ttl: 0, Contiguous allocation: 1
```

```
Lifetime: from 10:00:00 PDT Jul 4 1999 until 10:00:00 PDT Aug 1 1999
Uptime: 4d05h, Last Heard: 00:01:40
Announcement source: 128.102.84.134
Created by: sample 3136541828 3139561476 IN IP4 128.102.84.134
Phone number: Sample Digital Video Lab (555) 555-5555
Email: email1 <name@email.com>
URL: http://url.com/
Media: audio 20890 RTP/AVP 0
  Media group: 224.2.197.250, ttl: 127
  Attribute: ptime:40
Media: video 62806 RTP/AVP 31
  Media group: 224.2.190.243, ttl: 127
```

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

Table 61: show ip sap Field Descriptions

Field	Description
SAP Cache - 198 entries	Number of entries (sessions) in the cache.
Session Name:	Name of session.
Description:	Description of the session. Individual media may have their own Description field.
Group:	IP multicast group addresses used for this session. The 0.0.0.0 IP address is displayed if individual media define separate multicast groups.
ttl:	The time-to-live (TTL) value associated with the multicast groups.
Contiguous Allocation:	Number of continuously ascending IP multicast group addresses allocated to this session.
Lifetime:	Period of time during which this session is presumed to carry traffic in the network.
Uptime:	How long (in hours, minutes, and seconds) this announcement has been stored.
Last Heard:	How long ago (in hours, minutes, and seconds) this announcement was last heard. This time is always less than the timeout value configured using the **sap cache-timeout** command.
Announcement source:	IP address of the host from which this session announcement was received.
Created by:	Information for identifying and tracking the session announcement.
Phone number:	Telephone number of the person or entity responsible for the session.

Field	Description
Email:	E-mail address of the person or entity responsible for the session.
URL:	URL for the location where further information about this session can be found.
Media:	Indicates the media type (audio, video, or data), transport port that the medium stream is sent to, transport protocol used for these media (common values are User Datagram Protocol [UDP] and Real-Time Transport Protocol [RTP]/attribute-value pair [AVP]), and list of media formats that each media instance can use. The first media format is the default format. Format identifiers are specific to the transport protocol used.
Media group:	Indicates the IP multicast group address over which the media instance is sent.
Attribute:	Indicates attributes specific to each media instance.

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
ip sap cache-timeout	Limits how long a SAP cache entry stays active in the cache.
ip sap listen	Enables the Cisco IOS software to listen to session directory announcements.

show ip sdr

The **show ip sdr**command is replaced by the **show ip sap** command. See the description of the **show ip sap** command for more information.