IP Multicast Routing Commands

- clear ip mfib counters, on page 3
- clear ip mroute, on page 4
- clear ip pim snooping vlan, on page 5
- debug condition vrf, on page 6
- debug ip pim, on page 7
- debug ipv6 pim, on page 9
- device tracking export oper data, on page 11
- ip igmp filter, on page 12
- ip igmp max-groups, on page 13
- ip igmp profile, on page 15
- ip igmp snooping, on page 16
- ip igmp snooping last-member-query-count, on page 17
- ip igmp snooping querier, on page 19
- ip igmp snooping report-suppression, on page 21
- ip igmp snooping tcn flood, on page 22
- ip igmp snooping vlan mrouter, on page 24
- ip igmp snooping vlan static, on page 25
- ip mroute extend-timer, on page 26
- ip multicast auto-enable, on page 27
- ip multicast-routing, on page 28
- ip pim accept-register, on page 29
- ip pim bidir-enable, on page 30
- ip pim bsr-candidate, on page 31
- ip pim query-interval, on page 33
- ip pim rp-address, on page 34
- ip pim rp-candidate, on page 36
- ip pim send-rp-announce, on page 37
- ip pim snooping, on page 39
- ip pim snooping dr-flood, on page 40
- ip pim snooping vlan, on page 41
- ip pim spt-threshold, on page 42
- match message-type, on page 43
- match service-type, on page 44

- match service-instance, on page 45
- mrinfo, on page 46
- service-policy-query, on page 48
- service-policy, on page 49
- show ip igmp filter, on page 50
- show ip igmp profile, on page 51
- show ip igmp snooping, on page 52
- show ip igmp snooping groups, on page 54
- show ip igmp snooping mrouter, on page 56
- show ip igmp snooping querier, on page 57
- show ip mroute, on page 59
- show ip pim autorp, on page 67
- show ip pim bsr-router, on page 69
- show ip pim bsr, on page 70
- show ip pim interface df, on page 71
- show ip pim rp, on page 73
- show ip pim snooping, on page 76
- show ip pim tunnel, on page 79
- show mvpn vrfri, on page 81
- show platform software fed ip multicast groups, on page 82
- show platform software fed active ip multicast, on page 83
- show platform software fed ip multicast df, on page 85

clear ip mfib counters

To clear all the active IPv4 Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ip mfib counters** command in privileged EXEC mode.

clear ip mfib [**global** | **vrf** ***] **counters** [*group-address*] [*hostname* | *source-address*]

Syntax Description

global	(Optional) Resets the IP MFIB cache to the global default configuration.
vrf *	(Optional) Clears the IP MFIB cache for all VPN routing and forwarding instances.
group-address	(Optional) Limits the active MFIB traffic counters to the indicated group address.
hostname	(Optional) Limits the active MFIB traffic counters to the indicated host name.
source-address	(Optional) Limits the active MFIB traffic counters to the indicated source address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to reset all the active MFIB traffic counters for all the multicast tables:

```
# clear ip mfib counters
```

The following example shows how to reset the IP MFIB cache counters to the global default configuration:

```
# clear ip mfib global counters
```

The following example shows how to clear the IP MFIB cache for all the VPN routing and forwarding instances:

```
# clear ip mfib vrf * counters
```

clear ip mroute

To delete the entries in the IP multicast routing table, use the **clear ip mroute**command in privileged EXEC mode.

clear ip mroute [**vrf** *vrf-name*]{***** | *ip-address* | *group-address*}[*hostname* | *source-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
*****	Specifies all Multicast routes.
ip-address	Multicast routes for the IP address.
group-address	Multicast routes for the group address.
hostname	(Optional) Multicast routes for the host name.
source-address	(Optional) Multicast routes for the source address.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The *group-address* variable specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a group name or address, you can also enter the source argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

Example

The following example shows how to delete all the entries from the IP multicast routing table:

```
# clear ip mroute *
```

The following example shows how to delete all the sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources:

```
# clear ip mroute 224.2.205.42 228.3.0.0
```

clear ip pim snooping vlan

Note This command is not applicable on Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP- 2)

To delete the Protocol Independent Multicast (PIM) snooping entries on a specific VLAN, use the **clear ip pim snooping vlan** command in user EXEC or privileged EXEC mode.

clear ip pim snooping vlan *vlan-id* [**neighbor** | **statistics** | **mroute** [*source-ipgroup-ip*]]

Syntax Description

vlan *vlan-id*	VLAN ID. Valid values are from 1—4094.
neighbor	Deletes all the neighbors.
statistics	Deletes information about the VLAN statistics.
mroute *group-addr src-addr*	Deletes the mroute entries in the specified group and the source IP address.

Command Default

This command has no default settings.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Examples

This example shows how to clear the IP PIM-snooping entries on a specific VLAN:

```
Router# clear ip pim snooping vlan 1001
```

Related Commands

Command	Description
ip pim snooping	Enables PIM snooping globally.
show ip pim snooping	Displays information about IP PIM snooping.

debug condition vrf

To limit debug output to a specific virtual routing and forwarding (VRF) instance, use the **debug condition vrf** command in privileged EXEC mode. To remove the debug condition, use the **no** form of the command.

debug condition vrf {**default** | **global** | **green** | **name** {*vrf-name* | **green**}}

no debug condition vrf {**default** | **global** | **green** | **name** {*vrf-name* | **green**}}

Syntax Description

Syntax	Description
default	Specifies the default routing table.
global	Specifies the global routing table.
green	Specifies the VRF name.
name *vrf-name*	Specifies the name of the routing table.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Use this command to limit debug output to a single VRF.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Example

The following example shows how to limit debugging output to VRF red:

```
Device# debug condition vrf red
```

debug ip pim

To display PIM packets received and transmitted, as well as PIM related events, use the **debug ip pim** command in privileged EXEC mode. To disable the debug output, use the **no** form of the command.

debug ip pim [**vrf** *vrf-name*][*ip-address* | **atm** | **auto-rp** | **bfd** | **bsr** | **crimson** | **df** *rp-address* | **drlb** | **hello** | **timers**]

no debug ip pim [**vrf** *vrf-name*][*ip-address* | **atm** | **auto-rp** | **bfd** | **bsr** | **crimson** | **df** *rp-address* | **drlb** | **hello** | **timers**]

Syntax Description

Syntax	Description
vrf *vrf-name*	(Optional) Specifies the VPN Routing and Forwarding instance. This keyword overrides debugging of any VRFs specified in the **debug condition vrf** *vrf-name* command.
ip-address	(Optional) Specifies the IP group address.
atm	(Optional) Displays debugging information about PIM ATM signalling activity.
auto-rp	(Optional) Displays debugging information about Auto-RP information.
bfd	(Optional) Displays debugging information about BFD configuration.
bsr	(Optional) Displays debugging information about PIM Candidate-RP and BSR activity.
crimson	(Optional) Displays debugging information about Crimson database activity.
df *rp-address*	(Optional) Displays debugging information about PIM RP designated forwarder election activity.
drlb	(Optional) Displays debugging information about PIM designated router load-balancing activity.
hello	(Optional) Displays debugging information about PIM Hello packets received and sent.
timers	(Optional) Displays debugging information about PIM timer events.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

You can debug a maximum of 8 VRFs in a PIM at a time. To debug multiple VRFs at the same time, perform the following sequence of steps:

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

Example

The following example shows how to display the Crimson database activity:

```
Device# debug ip pim crimson
```

The following example shows how to debug the two VRFs red and green in a PIM at the same time:

```
Device# debug condition vrf red
Device# debug condition vrf green
Device# debug ip pim
```

debug ipv6 pim

To enable debugging on Protocol Independent Multicast (PIM) protocol activity, use the **debug ipv6 pim** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

```
debug ipv6 pim
[vrf vrf-name ]
[bfd interface-type interface-number |bsr |crimson |df-election [interface interface-type
interface-number | rp rp-address]|drlb|group group-address |interface interface-type
interface-number |limit [group-address ]|neighbor interface-type interface-number ]
```

```
no debug ipv6 pim
[vrf vrf-name ]
[bfd interface-type interface-number |bsr |crimson |df-election [interface interface-type
interface-number | rp rp-address]|drlb|group group-address |interface interface-type
interface-number |limit [group-address ]|neighbor interface-type interface-number ]
```

Syntax Description

Syntax	Description
vrf *vrf-name*	(Optional) Specifies the VPN Routing and Forwarding instance. This keyword overrides debugging of any VRFs specified in the **debug condition vrf** *vrf-name* command.
bfd	(Optional) Displays debugging information about BFD configuration.
bsr	(Optional) Displays debugging information about PIM Candidate-RP and BSR sent and received.
crimson	(Optional) Displays debugging information about Crimson database activity.
df-election	(Optional) Displays debugging information about PIM designated forwarder election activity.
drlb	(Optional) Displays debugging information about PIM designated router load-balancing activity.
group *group-address*	(Optional) Displays debugging information about group-related activity.
interface	(Optional) Displays debugging information about protocol activity of the specified interface.
limit	(Optional) Displays debugging information about interface limits.

Syntax	Description
neighbor	(Optional) Displays debugging information about PIM Hello messages received and sent.
interface-type interface-number	(Optional) Displays debugging information about the specified interface.
rp *rp-address*	(Optional) Displays debugging information about the specified RP.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

You can debug a maximum of 8 VRFs in a PIM at a time. To debug multiple VRFs at the same time, perform the following sequence of steps:

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

Example

The following example shows how to display the Crimson database activity:

```
Device# debug ipv6 pim crimson
```

The following example shows how to debug VRF red:

```
Device# debug vrf red ipv6 pim
```

device tracking export oper data

To export the IP and MAC databases for Switch Integrated Security Features to the Crimson database, use the **device-tracking export oper-data** command. To remove the configuration use the **no** form of the command.

device-tracking export oper-data [**enable** | **disable**]

Syntax Description

enable	Enables operational data export to the Crimson database.
disable	Disables operational data export to the Crimson database.

Command Default

Operational data export is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 17.14.1	This command was introduced.

Usage Guidelines

When the **device-tracking export oper-data enable** command is used:

- The IP and MAC address tables are not immediately repopulated with the current state of the SISF database. No events will be generated for the current database entries.
- Subsequent changes to MAC and IP address entries will be published in the IP and MAC address tables and event-queues.

When you disable the configuration using the **device-tracking export oper-data disable** command:

- All published entries are removed from the IP and MAC address tables in the Crimson database.
- Deletes events for all entries that are published through the relevant event-queue.
- Further updates are not published in either the tables or event-queues.

Example

The following example shows how to enable exporting of information to the Crimson database using the **device-tracking export oper-data enable** command:

```
Device(config)#device-tracking export oper-data enable
```

The following example shows how to disable exporting of information to the Crimson database using the **device-tracking export oper-data disable** command:

```
Device(config)#device-tracking export oper-data disable
```

ip igmp filter

To control whether or not all the hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface, use the **ip igmp filter** interface configuration command on the stack or on a standalone . To remove the specified profile from the interface, use the **no** form of this command.

ip igmp filter *profile number*
no ip igmp filter

Syntax Description

profile number	IGMP profile number to be applied. The range is 1—4294967295.

Command Default

No IGMP filters are applied.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more port interfaces, but one port can have only one profile applied to it.

Example

This example shows how to configure IGMP profile 40 to permit the specified range of IP multicast addresses, then shows how to apply that profile to a port as a filter:

```
(config)# ip igmp profile 40
(config-igmp-profile)# permit
(config-igmp-profile)# range 233.1.1.1 233.255.255.255
(config-igmp-profile)# exit
(config)# interface gigabitethernet1/0/2
(config-if)# switchport
*Jan  3 18:04:17.007: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down.
NOTE: If this message appears, this interface changes to layer 2, so that you can apply the
 filter.
(config-if)# ip igmp filter 40
```

You can verify your setting by using the **show running-config** command in privileged EXEC mode and by specifying an interface.

ip igmp max-groups

To set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table, use the **ip igmp max-groups** interface configuration command on the stack or on a standalone . To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

ip igmp max-groups {*max number* | **action** { **deny** | **replace**} }
no ip igmp max-groups {*max number* | **action**}

Syntax Description

max number	Maximum number of IGMP groups that an interface can join. The range is 0—4294967294. The default is no limit.
action deny	Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.
action replace	Replaces the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the IGMP snooping forwarding table.

Command Default

The default maximum number of groups is no limit.

After the learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny, and set the maximum group limit, the entries that were previously in the forwarding table are not removed, but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the drops the next IGMP report received on the interface.
- If you configure the throttling action as replace, and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {deny | replace}** command has no effect.

Example

The following example shows how to limit the number of IGMP groups that a port can join to 25:

```
(config)# interface gigabitethernet1/0/2
(config-if)# ip igmp max-groups 25
```

The following example shows how to configure the to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
(config)# interface gigabitethernet2/0/1
(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

ip igmp profile

To create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command on the stack or on a standalone . From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switch port. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*
no ip igmp profile *profile number*

Syntax Description

profile number	The IGMP profile number being configured. The range is from 1—4294967295.

Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create a profile by using these commands:

- **deny**—Specifies that matching addresses are denied; this is the default condition.
- **exit**—Exits from igmp-profile configuration mode.
- **no**—Negates a command or resets to its defaults.
- **permit**—Specifies that matching addresses are permitted.
- **range**—Specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Example

The following example shows how to configure IGMP profile 40, which permits the specified range of IP multicast addresses:

```
(config)# ip igmp profile 40
(config-igmp-profile)# permit
(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** command in privileged EXEC mode.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the stack or on a standalone . To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]
no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.

Command Default

IGMP snooping is globally enabled on the .

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable IGMP snooping:

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

The following example shows how to enable IGMP snooping on VLAN 1:

```
(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*
no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

Syntax Description

vlan *vlan-id*	(Optional) Sets the count value on a specific VLAN ID. The range is from 1—1001. Do not enter leading zeroes.
count	Interval at which query messages are sent, in milliseconds. The range is from 1—7. The default is 2.

Command Default

A query is sent every 2 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response is received to the last-member queries before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.

Note Do not set the count to 1 because the loss of a single packet (the query packet from the to the host or the report packet from the host to the) may result in traffic forwarding being stopped even if the receiver is still there. Traffic continues to be forwarded after the next general query is sent by the , but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to 1 last-member query interval (LMQI) value when the is processing more than one leave within an LMQI. In such a scenario, the average leave latency is determined by the (count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Example

The following example shows how to set the last member query count to 5:

```
(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]
no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. Ranges are 1—1001 and 1006—4094.
address *ip-address*	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
max-response-time *response-time*	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1—25 seconds.
query-interval *interval-count*	(Optional) Sets the interval between IGMP queriers. The range is 1—18000 seconds.
tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).
count *count*	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1—10.
interval *interval*	Sets the TCN query interval time. The range is 1—255.
timer expiry *expiry-time*	(Optional) Sets the length of time until the IGMP querier expires. The range is 60—300 seconds.
version *version*	(Optional) Selects the IGMP version number that the querier feature uses. Select either 1 or 2.

Command Default

The IGMP snooping querier feature is globally disabled on the .

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2), but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured, and is set to zero).

Non-RFC-compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable the IGMP snooping querier feature:

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

The following example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
(config)# ip igmp snooping querier max-response-time 25
```

The following example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
(config)# ip igmp snooping querier query-interval 60
```

The following example shows how to set the IGMP snooping querier TCN query count to 25:

```
(config)# ip igmp snooping querier tcn count 25
```

The following example shows how to set the IGMP snooping querier timeout value to 60 seconds:

```
(config)# ip igmp snooping querier timer expiry 60
```

The following example shows how to set the IGMP snooping querier feature to Version 2:

```
(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the stack or on a standalone . To disable IGMP report suppression, and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the sends the first IGMP report from all the hosts for a group to all the multicast routers. The does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the forwards only the first IGMPv1 or IGMPv2 report from all the hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

Example

The following example shows how to disable report suppression:

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

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip igmp snooping tcn flood

To enable flooding of multicast traffic during a spanning-tree Topology Change Notification (TCN) event for an interface after TCN flooding is explicitly disabled on the interface, use the **ip igmp snooping tcn flood** command in global configuration mode. To disable TCN flooding on an an interface, use the **no** form of this command.

ip igmp snooping tcn flood
no ip igmp snooping tcn flood

Syntax Description

This command has no arguments or keywords.

Command Default

TCN flooding is enabled on interfaces.

Command Modes

Global configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use this command to disable or enable TCN flooding on an interface. TCN flooding is enabled on all interfaces by default.

The Spanning Tree Protocol (STP) operates on the virtual port level. When a virtual port receives a TCN event, all interfaces that operate under that virtual port are identified, along with the bridge domain to which the interface belongs. Flooding is started to all interfaces on the bridge domain except the ones on which TCN flooding is explicitly disabled. This flooding can exceed the capacity of the virtual port and cause packet loss. Use the **no ip igmp snooping tcn flood** command to disable the flooding of multicast traffic on an interface during a spanning-tree TCN event .

Example

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

```
(config)#  int twe1/0/3
 (config-if)# no ip igmp snooping tcn flood
```

Example

The following example shows how to disable TCN flooding:

```
Device# sh pl so fed sw ac ip igmp snooping vlan 100
Vlan 100
---------
IGMPSN Enabled  : On
PIMSN Enabled   : Off
Flood Mode      : Off
Oper State      : Up
STP TCN Flood   : Off
Routing Enabled : On
PIM Enabled     : On
```

```
PVLAN           : No
In Retry        : 0x0
CCK Epoch       : 0x35
IOSD Flood Mode : Off
EVPN Proxy Enabled : Off
L3mcast Adj      :
Mrouter PortQ   :
TwentyFiveGigE1/0/2
Svl Link        : Enabled
Flood PortQ     : TwentyFiveGigE1/0/2
                  TwentyFiveGigE1/0/3
                  TwentyFiveGigE1/0/34
TCN PortQ     :
REP RI handle   : 0x0
```

After STP TCN Flood is set as on, the ports configured with no ip igmp snooping tcn flood gets excluded from TCN PortQ. The Ports getting flooded with multicast traffic are added in the respective local or remote TCN PortQ. In this example, interface TwentyFiveGigE1/0/3 is configured with no ip igmp snooping tcn flood command and gets excluded from TCN portQ.

```
Device(config) interface TwentyFiveGigE1/0/3
Device(config-if)# switchport access vlan 101
Device(config-if)# switchport mode access
Device(config-if)# no ip igmp snooping tcn flood
Device(config-if)# end

lannister#sh pl so fed sw ac ip igmp snooping vlan 101
Vlan 101
---------
IGMPSN Enabled  : On
PIMSN Enabled   : Off
Flood Mode      : Off
Oper State      : Up
STP TCN Flood   : On
Routing Enabled : On
PIM Enabled     : On
PVLAN           : No
In Retry        : 0x0
CCK Epoch       : 0x35
IOSD Flood Mode : Off
EVPN Proxy Enabled : Off
L3mcast Adj      :
Mrouter PortQ   : TwentyFiveGigE1/0/29
Svl Link        : Enabled
Flood PortQ     : TwentyFiveGigE1/0/29
                  TwentyFiveGigE1/0/2
                  TwentyFiveGigE1/0/3
TCN PortQ: TwentyFiveGigE1/0/2
TCN Remote Ports:TwentyFiveGigE2/0/2
REP RI handle: 0x0
```

ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the stack or on a standalone . To return to the default settings, use the **no** form of this command.

Command Default

By default, there are no multicast router ports.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

The following example shows how to configure a port as a multicast router port:

```
(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** global configuration command on the stack or on a standalone . To remove the port specified as members of a static multicast group, use the **no** form of this command.

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

Syntax Description

vlan-id	Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.
ip-address	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specifies the interface of the member port. The *interface-id* has these options: • *fastethernet interface number*—A Fast Ethernet IEEE 802.3 interface. • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0—128.

Command Default

By default, no ports are statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

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

```
(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1

Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip mroute extend-timer

This command introduces a mechanism to extend the expiry timer for newly created (S,G) mroutes if traffic stops within the first 2 minutes, preventing premature deletion and ensuring stability for infrequent or bursty traffic flows, while only applying to IPv4 ASM routes and not affecting SSM routes. To return to the default mode, use the **no** form of this command.

ip mroute extend-timer
no ip mroute extend-timer

Command Default

The feature is disabled by default and must be enabled using a specific CLI command.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 17.15.2	This command was introduced.

Usage Guidelines

Enabling this command automatically applies it to user VRFs, eliminating the need to enable it separately for each VRF. No explicit commands are required for VRF.

Examples

To enable the feature for extending the mroute expiry timer, use the following command in global configuration mode:

```
(config)# ip mroute extend-timer
```

This command ensures that the expiry timer for newly created (S,G) mroutes is extended if traffic stops within the first 2 minutes, preventing premature deletion.

To disable this feature, use the following command:

```
(config)# no ip mroute extend-timer
```

Disabling the feature reverts the mroute expiry behavior to default, where mroutes are aged out without extending the timer.

ip multicast auto-enable

To support authentication, authorization, and accounting (AAA) enabling of IP multicast, use the **ip multicast auto-enable** command. This command allows multicast routing to be enabled dynamically on dialup interfaces using AAA attributes from a RADIUS server. To disable IP multicast for AAA, use the **no** form of this command.

ip multicast auto-enable
no ip multicast auto-enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to enable AAA on IP multicast:

```
(config)# ip multicast auto-enable
```

ip multicast-routing

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

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

Syntax Description

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

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

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

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

Examples

The following example shows how to enable IP multicast routing:

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing
```

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

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

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim accept-register

To configure a candidate rendezvous point (RP) switch to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*}
no ip pim [**vrf** *vrf-name*] **accept-register**

Syntax Description

vrf *vrf-name*	(Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
list *access-list*	Specifies the *access-list* argument as a number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied. The range is 100—199 and the expanded range is 2000—2699. An IP-named access list can also be used.

Command Default

No PIM register filters are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list provided for the **ip pim accept-register** command should only filters IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is required, use the **ip multicast boundary** command instead.

Example

The following example shows how to permit register packets for a source address sending to any group range, with the exception of source address 172.16.10.1 sending to the SSM group range (232.0.0.0/8). These are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first-hop routers or switches.

```
(config)# ip pim accept-register list ssm-range
(config)# ip access-list extended ssm-range
(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
(config-ext-nacl)# permit ip any any
```

ip pim bidir-enable

To enable bidirectional Protocol Independent Multicast (bidirectional PIM), use the **ip pim bidir-enable** command in global configuration mode. To disable bidirectional PIM, use the **no** form of this command.

ip pim bidir-enable

no ip pim bidir-enable

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Command Default

The command is enabled.

Command Modes

Global configuration (config)

Usage Guidelines

When bidirectional PIM is disabled, the router will behave similarly to a router without bidirectional PIM support. The following conditions will apply:

- PIM hello messages sent by the router will not contain the bidirectional mode option.
- The router will not send designated forwarder (DF) election messages and will ignore DF election messages it receives.
- The **ip pim rp-address**, **ip pim send-rp-announce**, and **ip pim rp-candidate** global configuration commands will be treated as follows:
  - If these commands are configured when bidirectional PIM is disabled, bidirectional mode will not be a configuration option.
  - If these commands are configured with the bidirectional mode option when bidirectional PIM is enabled and then bidirectional PIM is disabled, these commands will be removed from the command-line interface (CLI). In this situation, these commands must be configured again with the bidirectional mode option when bidirectional PIM is reenabled.
- The **df** keyword for the **show ip pim interface** user EXEC or privileged EXEC command and **debug ip pim** privileged EXEC command is not supported.

The following example shows how to enable bidirectional PIM:

```
Device# enable
Device# configure terminal
Device(config)# ip pim bidir-enable
```

ip pim bsr-candidate

To configure the to be a candidate BSR, use the **ip pim bsr-candidate** command in global configuration mode. To remove the switch as a candidate BSR, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-id* [*hash-mask-length*] [*priority*]
no ip pim [**vrf** *vrf-name*] **bsr-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Configures the to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-id	ID of the interface on the from which the BSR address is derived to make it a candidate. This interface must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command. Valid interfaces include physical ports, port channels, and VLANs.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred.

Command Default

The is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command configures the to send BSR messages to all of its PIM neighbors, with the address of the designated interface as the BSR address.

This command should be configured on backbone s that have good connectivity to all parts of the PIM domain.

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) switches unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so, no pre-existing IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each switch that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Cisco always accept and process BSR messages. There is no command to disable this function.

Cisco perform the following steps to determine which C-RP is used for a group:

- A long match lookup is performed on the group prefix that is announced by the BSR C-RPs.
- If more than one BSR-learned C-RP is found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate** command) is preferred.
- If more than one BSR-learned C-RP has the same priority, the BSR hash function is used to select the RP for a group.
- If more than one BSR-learned C-RP returns the same hash value derived from the BSR hash function, the BSR C-RP with the highest IP address is preferred.

Example

The following example shows how to configure the IP address of the on Gigabit Ethernet interface 1/0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim query-interval

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

ip pim query-interval *period* **[msec]**
no ip pim query-interval

Syntax Description

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

Command Default

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

Command Modes

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

Command History

Release	Modification
Cisco IOS XE 17.16.1	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

ip pim rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**] [**bidir**]

no ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the static group-to-RP mapping be associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the vrf-name argument.
rp-address *rp-address*	IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.
access-list	(Optional) Number or name of a standard access list that defines the multicast groups to be statically mapped to the RP. **Note** If no access list is defined, the RP will map to all multicast groups
override	(Optional) Specifies that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
bidir	(Optional) Specifies that the static group-to-RP mapping be applied to a bidirectional PIM RP. If the command is configured without the **bidir** keyword, the groups will operate in sparse mode. **Note** The **bidir** keyword is available as an optional keyword only if bidirectional PIM has been enabled using the **ip pim bidir-enable** command.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Command Default

No PIM static group-to-RP mappings are configured.

Command Modes

Global configuration (config)

Usage Guidelines

Under PIM, multicast groups in sparse mode (PIM-SM) or bidirectional mode (bidirectional PIM) use RPs to connect sources and receivers. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

The Cisco IOS software learns the mode and RP addresses of multicast groups through the following three mechanisms: static group-to-RP mapping configurations, Auto-RP, and bootstrap router (BSR).

Use the **ip pim rp-address** command to statically define the RP address for PIM-SM or bidirectional PIM groups (an **ip pim rp-address** command configuration is referred to as a static group-to-RP mapping).

You can configure a single RP for more than one group using an access list. If no access list is specified, the static RP will map to all multicast groups.

You can configure multiple RPs, but only one RP per group range.

If multiple **ip pim rp-address** commands are configured, the following rules apply:

- Highest RP IP address selected regardless of reachability: If a multicast group is matched by the access list of more than one configured **ip pim rp-addres**s command, then the RP for the group is determined by the RP with the highest RP address configured.
- One RP address per command: If multiple **ip pim rp-address** commands are configured, each static group-to-RP mapping must be configured with a unique RP address (if not, it will be overwritten).This restriction also means that only one RP address can be used to provide RP functions for either sparse mode or bidirectional mode groups. If you want to configure static group-to-RP mappings for both bidirectional and sparse mode, the RP addresses must be unique for each mode.
- One access list per command: If multiple **ip pim rp-address** commands are configured, only one access list can be configured per static group-to-RP mapping. An access list cannot be reused with other static group-to-RP mappings configured on a router.

If dynamic and static group-to-RP mappings are used together, the following rule applies to a multicast group: Dynamic group-to-RP mappings take precedence over static group-to-RP mappings--unless the **override** keyword is used.

The following example shows how to set the bidirectional PIM RP address to 172.16.0.2 for the multicast range 239/8:

```
Device(config)# access list 10 239.0.0.0 0.255.255.255
Device(config)# ip pim rp-address 172.16.0.2 10 bidir
```

ip pim rp-candidate

To configure the to advertise itself to the BSR as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove the as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]
no ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the switch to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-id	ID of the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.
group-list *access-list-number*	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.

Command Default

The is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Use this command to configure the to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.

This command should be configured on backbone s that have good connectivity to all parts of the PIM domain.

The IP address associated with the interface specified by *interface-id* will be advertised as the C-RP address.

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

If the optional **group-list** keyword and *access-list-number* argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.

Example

The following example shows how to configure the switch to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 1/0/1.

```
(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

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

ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id* **scope** *ttl-value* [**group-list** *access-list-number*] [**interval** *seconds*] [**bidir**]
no ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id*

Syntax Description

vrf *vrf-name*	(Optional) Uses Auto-RP to configure groups for which the device will act as a rendezvous point (RP) for the *vrf-name* argument.
interface-id	Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.
scope *ttl-value*	Specifies the time-to-live (TTL) value in hops that limits the number of Auto-RP announcements. Enter a hop count that is high enough to ensure that the RP-announce messages reach all the mapping agents in the network. There is no default setting. The range is 1—255.
group-list *access-list-number*	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address. Enter an IP standard access list number from 1—99. If no access list is configured, the RP is used for all groups.
interval *seconds*	(Optional) Specifies the interval between RP announcements, in seconds. The total hold time of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds. The range is 1—16383.
bidir	(Optional) Indicates that the multicast groups specified by the access-listargument are to operate in bidirectional mode. If the command is configured without this keyword, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).

Command Default

Auto-RP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Gibraltar 16.12.1	This command was modified. The **bidir** keyword was added.

Usage Guidelines

Enter this command on the device that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

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

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

Example

The following example shows how to configure the device to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the switch wants to be identified as RP is the IP address associated with Gigabit Ethernet interface 1/0/1 at an interval of 120 seconds:

```
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval
 120
```

ip pim snooping

Note This command is not applicable on Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP- 2)

To enable Protocol Independent Multicast (PIM) snooping globally, use the **ip pim snooping** command in global configuration mode. To disable PIM snooping globally, use the **no** form of this command.

ip pim snooping
no ip pim snooping

Syntax Description

This command has no arguments or keywords.

Command Default

PIM snooping is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

When you disable PIM snooping globally, PIM snooping is disabled on all the VLANs.

Examples

The following example shows how to enable PIM snooping globally:

```
ip pim snooping
```

The following example shows how to disable PIM snooping globally:

```
no ip pim snooping
```

Related Commands

Command	Description
clear ip pim snooping	Deletes PIM snooping on an interface.
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping dr-flood

Note This command is not applicable on Cisco Catalyst 9600 Series Supervisor 2 Module (C9600-SUP- 2)

To enable flooding of packets to the designated router, use the **ip pim snooping dr-flood** command in global configuration mode. To disable the flooding of packets to the designated router, use the **no** form of this command.

ip pim snooping dr-flood
no ip pim snooping dr-flood

Syntax Description

This command has no arguments or keywords.

Command Default

The flooding of packets to the designated router is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

Enter the **no ip pim snooping dr-flood** command only on switches that have no designated routers attached.

The designated router is programmed automatically in the (S,G) O-list.

Examples

The following example shows how to enable flooding of packets to the designated router:

```
ip pim snooping dr-flood
```

The following example shows how to disable flooding of t packets to the designated router:

```
no ip pim snooping dr-flood
```

Related Commands

Command	Description
clear ip pim snooping	Deletes PIM snooping on an interface.
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping vlan

Note This command is not applicable on Cisco Catalyst 9600 Series Supervisor 2 Module (C9600-SUP- 2)

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

ip pim snooping vlan *vlan-id*
no ip pim snooping vlan *vlan-id*

Syntax Description

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

Command Default

PIM snooping is disabled on an interface.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

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

Examples

This example shows how to enable PIM snooping on a VLAN interface:

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

This example shows how to disable PIM snooping on a VLAN interface:

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

Related Commands

Command	Description
clear ip pim snooping	Deletes PIM snooping on an interface.
ip pim snooping	Enables PIM snooping globally.
show ip pim snooping	Displays information about IP PIM snooping.

ip pim spt-threshold

To specify the threshold that must be reached before moving to shortest-path tree (spt), use the **ip pim spt-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

ip pim {*kbps* | **infinity**} [**group-list** *access-list*]
no ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

Syntax Description

kbps	Threshold that must be reached before moving to shortest-path tree (spt). 0 is the only valid entry even though the range is 0 to 4294967. A 0 entry always switches to the source-tree.
infinity	Specifies that all the sources for the specified group use the shared tree, never switching to the source tree.
group-list *access-list*	(Optional) Specifies an access list number or a specific access list that you have created by name. If the value is 0 or if the **group-list** *access-list* option is not used, the threshold applies to all the groups.

Command Default

Switches to the PIM shortest-path tree (spt).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to make all the sources for access list 16 use the shared tree:

```
(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

To set a message type to match a service list, use the **match message-type** command.

match message-type {**announcement** | **any** | **query**}

Syntax Description

announcement	Allows only service advertisements or announcements for the .
any	Allows any match type.
query	Allows only a query from the client for a certain in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created, and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each one having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Note It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the announcement message type to be matched:

```
(config-mdns-sd-sl)# match message-type announcement
```

match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

match service-type *line*

Syntax Description

line	Regular expression to match the service type in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the value of the mDNS service type string to match:

```
(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match service-instance

To set a service instance to match a service list, use the **match service-instance** command.

match service-instance *line*

Syntax Description

line	Regular expression to match the service instance in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the service instance to match:

```
(config-mdns-sd-sl)# match service-instance servInst 1
```

mrinfo

To query which neighboring multicast routers or multilayer switches are acting as peers, use the **mrinfo** command in user EXEC or privileged EXEC mode.

mrinfo [**vrf** *route-name*] [*hostname* | *address*] [*interface-id*]

Syntax Description

vrf *route-name*	(Optional) Specifies the VPN routing or forwarding instance.
hostname | *address*	(Optional) Domain Name System (DNS) name or IP address of the multicast router or multilayer switch to query. If omitted, the switch queries itself.
interface-id	(Optional) Interface ID.

Command Default

The command is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers or switches are peering with multicast routers or switches. Cisco routers supports **mrinfo** requests from Cisco IOS Release 10.2.

You can query a multicast router or multilayer switch using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Example

The following is the sample output from the **mrinfo** command:

```
# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

Note The flags indicate the following:

- P: prune-capable
- M: mtrace-capable
- S: Simple Network Management Protocol-capable
- A: Auto RP capable

service-policy-query

To configure the service-list query periodicity, use the **service-policy-query** command. To delete the configuration, use the **no** form of this command.

service-policy-query [*service-list-query-name service-list-query-periodicity*]
no service-policy-query

Syntax Description

service-list-query-name service-list-query-periodicity	(Optional) Service-list query periodicity.

Command Default

Disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Since there are devices that do not send unsolicited announcements and to force such devices the learning of services and to keep them refreshed in the cache, this command contains an active query feature that ensures that the services listed in the active query list are queried.

Example

This example shows how to configure service list query periodicity:

```
(config-mdns)# service-policy-query sl-query1 100
```

service-policy

To apply a filter on incoming or outgoing service-discovery information on a service list, use the **service-policy** command. To remove the filter, use the **no** form of this command.

service-policy *service-policy-name* {**IN** | **OUT**}
no service-policy *service-policy-name* {**IN** | **OUT**}

Syntax Description

IN	Applies a filter on incoming service-discovery information.
OUT	Applies a filter on outgoing service-discovery information.

Command Default

Disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to apply a filter on incoming service-discovery information on a service list:

```
(config-mdns)#  service-policy serv-pol1 IN
```

show ip igmp filter

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

show ip igmp [**vrf** *vrf-name*] **filter**

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.

Command Default

IGMP filters are enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The **show ip igmp filter** command displays information about all filters defined on the .

Example

The following example shows the sample output from the **show ip igmp filter** command:

```
# show ip igmp filter

IGMP filter enabled
```

show ip igmp profile

To display all the configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** command in privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **profile** [*profile number*]

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
profile number	(Optional) IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all the IGMP profiles are displayed.

Command Default

IGMP profiles are undefined by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

None

Examples

The following example shows the output of the **show ip igmp profile** command for profile number 40 on the :

```
# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

The following example shows the output of the **show ip igmp profile** command for all the profiles configured on the :

```
# show ip igmp profile

IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

show ip igmp snooping

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

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description

groups	(Optional) Displays the IGMP snooping multicast table.
mrouter	(Optional) Displays the IGMP snooping multicast router ports.
querier	(Optional) Displays the configuration and operation information for the IGMP querier.
vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays operational state information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Examples

The following is a sample output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                       : Enabled
```

```
IGMPv2 immediate leave              : Disabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
```

The following is a sample output from the **show ip igmp snooping** command. It displays snooping characteristics for all the VLANs on the :

```
# 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
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                       : Enabled
IGMPv2 immediate leave              : Disabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Vlan 2:
--------
IGMP snooping                       : Enabled
IGMPv2 immediate leave              : Disabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
-
.
.
.
```

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the or the multicast information, use the **show ip igmp snooping groups** command in privileged EXEC mode.

show ip igmp snooping groups [**vlan** *vlan-id*] [[**count**] | *ip_address*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.
count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
ip_address	(Optional) Characteristics of the multicast group with the specified group IP address.

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Examples

The following is a sample output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the .

```
# show ip igmp snooping groups

Vlan      Group          Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4      igmp                    Gi1/0/11
1         224.1.4.5      igmp                    Gi1/0/11
2         224.0.1.40     igmp        v2          Gi1/0/15
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3      igmp        v2          Gi2/0/1, Gi2/0/2
```

The following is a sample output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the .

```
# show ip igmp snooping groups count

Total number of multicast groups: 2
```

The following is a sample output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
# show ip igmp snooping groups vlan 104 224.1.4.2

Vlan      Group          Type        Version     Port List
```

```
------------------------------------------------------------
104        224.1.4.2       igmp         v2           Gi2/0/1, Gi1/0/15
```

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** command in privileged EXEC mode.

show ip igmp snooping mrouter [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive, for example, if you enter | exclude output, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Example

The following is a sample output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the :

```
# show ip igmp snooping mrouter

Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier that is configured on a , use the **show ip igmp snooping querier**command in user EXEC mode.

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.
detail	(Optional) Displays detailed IGMP querier information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 .

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the , the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier was detected in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the querier (if any) that is configured in the VLAN

Expressions are case sensitive, for example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Examples

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

```
> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
--------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

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

```
> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP  querier status

-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP  querier status
-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

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.
vrf *	(Optional) Specifies all VRF instances.
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 device.
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

The **show ip mroute** command displays all entries in the mroute table.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Usage Guidelines

Use the **show ip mroute** command to display information about mroute entries in the mroute table. The asterisk (*) refers to all source addresses. In this case, using asterisk will display the information of all the VRFs related to multicast routing tables.

Example

The following example shows the sample output from the **show ip mroute** command:

```
Device# 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:

```
Device# 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 example shows the sample output from the **show ip mroute vrf *** command:

```
Device# show ip mroute vrf *
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag, l - LISP Decap Refcnt Contributor
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
                          t - LISP transit group
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

VRF IPv4 default
(100.99.99.99, 232.101.100.138), 1w1d/00:02:58, flags: sT
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse, 1w1d/00:02:58, flags:

(100.99.99.99, 232.101.100.157), 1w1d/00:03:27, flags: sT
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse, 1w1d/00:03:27, flags:

(100.88.88.88, 232.134.100.138), 1w1d/00:01:54, flags: sT
  Incoming interface: Ethernet0/0, RPF nbr 40.10.2.1
  Outgoing interface list:
    Null0, Forward/Dense, 1w1d/stopped, flags:
(100.88.88.88, 232.134.100.157), 1w1d/00:01:54, flags: sT
  Incoming interface: Ethernet0/0, RPF nbr 40.10.2.1
  Outgoing interface list:
    Null0, Forward/Dense, 1w1d/stopped, flags:

(*, 224.0.1.40), 1w1d/00:02:53, RP 0.0.0.0, flags: DP
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null

VRF red
(*, 225.64.64.1), 1w1d/00:03:23, RP 5.5.5.5, flags: Sl
  Incoming interface: LISP0.101, RPF nbr 100.88.88.88
```

```
  Outgoing interface list:
    LISP0.101, (100.99.99.99, 232.101.100.157), Forward/Sparse, 1w1d/stopped, flags:

(*, 225.32.32.32), 1w1d/00:03:05, RP 5.5.5.5, flags: Sl
  Incoming interface: LISP0.101, RPF nbr 100.88.88.88
  Outgoing interface list:
    LISP0.101, (100.99.99.99, 232.101.100.138), Forward/Sparse, 1w1d/stopped, flags:
```

Table 1: 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 device 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 device 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 device 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 device 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 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 device immediately switches to the shortest path source tree when traffic from a new source is received. • 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” device. A “turnaround” device is located at the intersection of a shared path (*, G) tree and the shortest path from the source to the RP.

Field	Description
	• 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 device (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.
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.

Field	Description
(*, 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 device 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 device. For devices and access servers operating in sparse mode, this address is always 224.0.0.0.
flags:	Information about the entry.
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 device to the source. Tunneling indicates that this device 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.

show ip pim autorp

To display global information about auto-rp, use the **show ip pim autorp** command in privileged EXEC mode.

show ip pim [**vrf** { *vrf-name* | ***** }] **autorp**

vrf *vrf-name*	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf *	(Optional) Specifies all the VRFs instances.

Command Default

Auto RP is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Usage Guidelines

This command displays whether auto-rp is enabled or disabled. The asterisk (*) refers to all VRFs. In this case, using asterisk will display the autorp information, for all applicable VRFs.

Example

The following command output shows that Auto RP is enabled:

```
# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

The following example shows the sample output from the **show ip pim vrf * autorp** command:

```
Device#show ip pim vrf * autorp
VRF IPv4 default

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on Loopback0.
  AutoRP groups over sparse mode interface is enabled

PIM AutoRP Statistics: Sent/Received
  RP Announce: 453427/0, RP Discovery: 0/152194

VRF ENG
```

```
AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 1500.
  224.0.1.40 is joined on GigabitEthernet4.
  AutoRP groups over sparse mode interface is enabled

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/151143, RP Discovery: 151923/0
```

show ip pim bsr-router

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** { *vrf-name* | ***** }] **bsr-router**

vrf *vrf-name*	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf *	(Optional) Specifies all the VRFs instances.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Usage Guidelines

In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information. The asterisk (*) refers to all VRFs. In this case, using asterisk will display the BSR router information, for all applicable VRFs.

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

```
# 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
```

show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** { *vrf-name* | ***** }] **bsr**

vrf *vrf-name*	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf *	(Optional) Specifies all the VRFs instances.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Usage Guidelines

In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information. The asterisk (*) refers to all VRFs. In this case, using asterisk will display the BSR protocol information, for all applicable VRFs.

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

```
# show ip pim bsr

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
```

show ip pim interface df

To display information about the elected designated forwarder (DF) for each rendezvous point (RP) on an interface configured for Bidirectional Protocol Independent Multicast (PIM), use the **show ip pim interface df** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** { *vrf-name* | ***** }] **interface** [*interface-type* | *interface-name*] **df** [*rp-address*]

vrf *vrf-name*	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf *	(Optional) Specifies all the VRFs instances.
interface [*interface-type* | *interface-name*]	Specifies the interface type or the interface number.
rp-address	(Optional) Specifies the RP IP address.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Command Default

If no interface is specified, all interfaces are displayed. The asterisk (*) refers to all VRFs. In this case, using asterisk will display information of the designated forwarder for each rendezvous point on an interface, for all applicable VRFs.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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

```
Device# 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
```

The following is sample output from the **show ip pim interface df** command when an interface is specified:

```
Device# 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 following table gives the output field descriptions for the **show ip pim interface df** command:

Field	Description
RP	IP address of the RP.
DF Winner	IP address of the elected DF.
Metric	Unicast routing metric to the RP announced by the DF.
Uptime	Length of time the RP has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.
State	Indicates whether the specified interface is an elected DF.
Offer count is	Number of PIM DF election offer messages that the router has sent out the interface during the current election interval.
Current DF IP address	IP address of the current DF.
DF winner uptime	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.

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** [**elected** | **in-use**] | **metric**] [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf *	(Optional) Specifies all the VRFs instances.
mapping [**elected** | **in-use**]	(Optional) Displays all group-to-RP mappings of which the router is aware. (either configured or learned from Auto-RP) • **elected**- Displays elected Auto RPs. • **in-use**- Displays learned RPs in-use.
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) Specifies the RP IP address.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Command Default

If no RP is specified, all active RPs are displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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."

The asterisk (*) refers to all VRFs. In this case, using asterisk will display information related to active RPs that are cached with associated multicast routing entries, for all applicable VRFs.

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

```
Device# 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:

```
Device# 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:

```
Device# 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 following is sample output from the **show ip pim vrf * rp mapping** command:

```
Device# show ip pim vrf * rp mapping
VRF IPv4 default
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)

Group(s) 224.0.0.0/4
  RP 3.3.3.3 (?), v2v1
```

```
    Info source: 2.2.2.2 (?), elected via Auto-RP
         Uptime: 4w3d, expires: 00:02:27
Group(s): 224.0.0.0/4, Static
    RP: 1.2.3.4 (?)
Acl: abc, Static
    RP: 1.1.1.1 (?)

VRF ENG
PIM Group-to-RP Mappings
This system is an RP-mapping agent

Group(s) 224.0.0.0/4
  RP 8.8.8.8 (?), v2v1
    Info source: 8.8.8.8 (?), elected via Auto-RP
         Uptime: 4w3d, expires: 00:02:07
```

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** | **statistics** | **mroute** [*source-ipgroup-ip*]]

Syntax Description

vlan *vlan-id*	Displays information for a specific VLAN; Valid values are from 1—4094.
neighbor	(Optional) Displays information about the neighbor database.
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
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Examples

The following example shows how to display information about the global status:

```
Router# show ip pim snooping

Global runtime mode: Enabled
Global admin mode  : Enabled
DR Flooding status : Disabled
SGR-Prune Suppression: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 1001
```

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

```
Router# show ip pim snooping vlan 1001

4 neighbors (0 DR priority incapable, 4 Bi-dir incapable)
5000 mroutes, 0 mac entries
DR is 10.10.10.4
RP DF Set:
QinQ snooping : Disabled
```

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

```
Router# show ip pim snooping vlan 1001 neighbor

IP Address       Mac address     Port            Uptime/Expires    Flags
VLAN 1001: 3 neighbors
10.10.10.2        000a.f330.344a  Po128           02:52:27/00:01:41
10.10.10.1        000a.f330.334a  Hu1/0/7         04:54:14/00:01:38
10.10.10.4        000a.f330.3c00  Hu1/0/1         04:53:45/00:01:34 DR
```

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

```
Router# show ip pim snooping vlan 1001 statistics

PIMv2 statistics:
Total                                          : 56785
Process Enqueue                                : 56785
Process PIMv2 input queue current outstanding  : 0
Process PIMv2 input queue max size reached     : 110
Error - Global Process State not RUNNING       : 0
Error - Process Enqueue                        : 0
Error - Drops                                  : 0
Error - Bad packet floods                      : 0
Error - IP header generic error                : 0
Error - IP header payload len too long         : 0
Error - IP header payload len too short        : 0
Error - IP header checksum                     : 0
Error - IP header dest ip not 224.0.0.13       : 0
Error - PIM header payload len too short       : 0
Error - PIM header checksum                    : 0
Error - PIM header checksum in Registers       : 0
Error - PIM header version not 2               : 0
```

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

```
Router# show ip pim snooping vlan 10 mroute

Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune

VLAN 1001: 5000 mroutes
(*, 225.0.1.0), 00:14:54/00:02:59
  10.10.10.120->10.10.10.105, 00:14:54/00:02:59, J
  Downstream ports: Po128
  Upstream   ports: Hu1/0/7
  Outgoing   ports: Hu1/0/7 Po128

(11.11.11.10, 225.0.1.0), 00:14:54/00:02:59
  10.10.10.130->10.10.10.120, 00:14:54/00:02:59, SGR-P
  Downstream ports:
  Upstream   ports: Hu1/0/7
  Outgoing   ports:

(*, 225.0.5.0), 00:14:53/00:02:57
  10.10.10.105->10.10.10.10, 00:14:53/00:02:57, J
  Downstream ports: Po128
  Upstream   ports: Hu1/0/7
  Outgoing   ports: Hu1/0/7 Po128

(11.11.11.10, 225.0.5.0), 00:14:53/00:02:57
  10.10.10.105->10.10.10.130, 00:14:53/00:02:57, SGR-P
```

```
  Downstream ports:
  Upstream   ports: Hu1/0/7
  Outgoing   ports:
Number of matching mroutes found: 4
```

This example shows how to display 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 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 2: show ip pim snooping Field Descriptions

Field	Description
Downstream ports	Ports on which PIM joins were received.
Upstream ports	Ports towards RP and source.
Outgoing ports	List of all upstream and downstream ports for the multicast flow.

Related Commands

Command	Description
clear ip pim snooping vlan	Deletes PIM snooping on an interface.
ip pim snooping	Enables PIM snooping globally.
ip pim snooping vlan	Enables PIM snooping on an interface.

show ip pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and decapsulation tunnels on an interface, use the **show ip pim tunnel** command.

show ip pim [**vrf** { *vrf-name* | ***** }] **tunnel** [**Tunnel** *interface-number* | **verbose**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
vrf *	(Optional) Specifies all the VRFs instances.
Tunnel *interface-number*	(Optional) Specifies the tunnel interface number.
verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	The asterisk (*) was introduced to display information related to all VRF instances.

Usage Guidelines

Use the **show ip pim tunnel** 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 (through 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—but 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 appears when a PIM tunnel interface is created:

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

The asterisk (*) refers to all VRFs. In this case, using asterisk will display information related to tunnel interfaces, for all applicable VRFs.

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

```
# show ip pim tunnel

Tunnel0
   Type  : PIM Encap
  RP    : 70.70.70.1*
  Source: 70.70.70.1
Tunnel1*
  Type  : PIM Decap
  RP    : 70.70.70.1*
  Source: -R2#
```

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

show mvpn vrfri

To display information about the VRF route import used for setting up the Multiprotocol Label Switching (MPLS) Multicast Label Distribution Protocol (MLDP), use the **show mvpn vrfri**command in user EXEC mode.

show mvpn vrfi

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command is introduced.

Usage Guidelines

The command displays information about the VRF route import attribute used for setting up the MPLS MLDP environment for the specific RPF neighbor and source.

Note This is applicable to MLDP based MVPN Profile 14 - Partitioned MDT in an Inter-AS MPLS VPN network deployed with Option B model to exchange routes across the autonomous systems.

Example

The following example is a sample output from the **show mvpn vrfri** command:

```
Device#show mvpn vrfri
MVPN RPF neighbor VRF-Route Import database:

VRF: 2, Source: 192.168.2.1, RPF: 1.1.1.1, VRF RI: 10.1.1.1, Uptime: 20:27:55
VRF: 2, Source: 192.168.3.1, RPF: 1.1.1.1, VRF RI: 10.1.1.1, Uptime: 20:27:55
VRF: 2, Source: 192.168.4.1, RPF: 1.1.1.1, VRF RI: 10.1.1.2, Uptime: 00:04:48
VRF: 2, Source: 192.168.5.1, RPF: 1.1.1.1, VRF RI: 10.1.1.2, Uptime: 00:04:48
VRF: 2, Source: 192.168.6.1, RPF: 1.1.1.1, VRF RI: 10.1.1.2, Uptime: 00:04:48
```

show platform software fed ip multicast groups

To display platform-dependent IP multicast groups information, use the **show platform software fed ip multicast groups** command in privileged EXEC mode.

show platform software fed { **active** | **standby** } **ip multicast groups** [**vrf-id** *vrf-id* | **vrf-name** *vrf-name*] [*group-address* [**source** *source-address*] [**detail**] | **count** | **summary**]

Syntax Description

{ **active** | **standby** }	The device for which you want to display information. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
vrf *vrf-id*	(Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) ID.
vrf *vrf-name*	(Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) name.
group-address	(Optional) Specifies the IP Multicast Group Address.
source *source-address*	(Optional) Specifies the IP Multicast Source Address
detail	(Optional) Specifies the IP Multicast group detail.
count	(Optional) Specifies the IP Multicast group count.
summary	(Optional) Specifies the Multicast group summary.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced

Command Modes

Privileged EXEC (#)

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

show platform software fed active ip multicast

To display platform-dependent IP multicast tables and other information, use the **show platform software fed active ip multicast** command in privileged EXEC mode.

show platform software fed {**active** | **standby**} **ip multicast** {**groups** | [**detail**] | **interfaces** | **retry**}

Syntax Description

{**active** | **standby** }	The device for which you want to display information. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
groups	Displays the IP multicast routes per group.
interfaces	Displays the IP multicast interfaces.
retry	Displays the IP multicast routes in the retry queue.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Example

The following example shows how to display platform IP multicast routes per group:

```
# show platform software fed active ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6  flags:  C
No RPF interface.
Number of OIF: 0
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
----------
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0
```

```
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==================================================================

<output truncated>
```

show platform software fed ip multicast df

To display information about platform-dependent IP multicast designated forwarders (DF), use the **show platform software fed ip multicast df** command in privileged EXEC mode.

show platform software fed {**active** | **standby**} **ip multicast df**[**vrf-id** *vrf-id* | **vrf-name** *vrf-name*][*df-index*]

Syntax Description

{**active** | **standby** }	The device for which you want to display information. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
vrf-id *vrf-id*	(Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) ID.
vrf *vrf-name*	(Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) name.
df-index	(Optional) Specifies the DF index.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

The following is sample output from the show platform software fed ip multicast df command:

```
Device# show platform software fed active ip multicast df
VRF-ID  DF-Index        Ref-Count       DF Set
================================================
2       1               1               Vlan254
                                        Vlan186
                                        Vlan305
                                        Vlan135
                                        Tunnel4
                                        Null0
```