



IP Multicast Routing

- [cache-memory-max](#), on page 3
- [clear ip mfib counters](#), on page 4
- [clear ip mroute](#), on page 5
- [ip igmp filter](#), on page 6
- [ip igmp max-groups](#), on page 7
- [ip igmp profile](#), on page 9
- [ip igmp snooping](#), on page 10
- [ip igmp snooping last-member-query-count](#), on page 11
- [ip igmp snooping querier](#), on page 13
- [ip igmp snooping report-suppression](#), on page 15
- [ip igmp snooping vlan mrouter](#), on page 16
- [ip igmp snooping vlan static](#), on page 17
- [ip multicast auto-enable](#), on page 18
- [ip pim accept-register](#), on page 19
- [ip pim bsr-candidate](#), on page 20
- [ip pim rp-candidate](#), on page 22
- [ip pim send-rp-announce](#), on page 23
- [ip pim spt-threshold](#), on page 25
- [match message-type](#), on page 26
- [match service-type](#), on page 27
- [match service-instance](#), on page 28
- [mrinfo](#), on page 29
- [redistribute mdns-sd](#), on page 31
- [service-list mdns-sd](#), on page 32
- [service-policy-query](#), on page 33
- [service-routing mdns-sd](#), on page 34
- [service-policy](#), on page 35
- [show ip igmp filter](#), on page 36
- [show ip igmp profile](#), on page 37
- [show ip igmp snooping](#), on page 38
- [show ip igmp snooping groups](#), on page 40
- [show ip igmp snooping mrouter](#), on page 42
- [show ip igmp snooping querier](#), on page 43

- [show ip pim autorp](#), on page 45
- [show ip pim bsr-router](#), on page 46
- [show ip pim bsr](#), on page 47
- [show ip pim tunnel](#), on page 48
- [show mdns cache](#), on page 50
- [show mdns requests](#), on page 52
- [show mdns statistics](#), on page 53
- [show platform software fed switch ip multicast](#), on page 54

cache-memory-max

To set the percentage of the system memory for cache, use the **cache-memory-max** command. To remove the percentage of system memory for cache, use the **no** form of this command.

cache-memory-max *cache-config-percentage*
no cache-memory-max *cache-config-percentage*

Syntax Description

cache-config-percentage A percentage of the system memory for cache.

Command Default

By default, the system memory is set to 10 percent.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The number of services learned in a network could be large, so there is an upper limit on the amount of cache memory that can be used.



Note

You can override the default value by using this command.

When you try to add new records, and the cache is full, the records in the cache that are close to expiring are deleted to provide space for the new records.

Example

This example sets 20 percent of the system memory for cache:

```
Device(config-mdns)# cache-memory-max 20
```

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.
	<i>group-address</i>	(Optional) Limits the active MFIB traffic counters to the indicated group address.
	<i>hostname</i>	(Optional) Limits the active MFIB traffic counters to the indicated host name.
	<i>source-address</i>	(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 3.3SE Cisco IOS XE 3.3SE	This command was introduced.

Example

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

```
Device# clear ip mfib counters
```

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

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

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

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

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE
		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:

```
Device# 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:

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

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 device stack or on a standalone device. 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 3.3SECisco IOS XE 3.3SE	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 device port interfaces, but one port can have only one profile applied to it.

Example

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 device stack or on a standalone device. 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	<table> <tr> <td><i>max number</i></td><td>Maximum number of IGMP groups that an interface can join. The range is 0—4294967294. The default is no limit.</td></tr> <tr> <td>action deny</td><td>Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.</td></tr> <tr> <td>action replace</td><td>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.</td></tr> </table>	<i>max number</i>	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.
<i>max number</i>	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	<p>The default maximum number of groups is no limit.</p> <p>After the device 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.</p>						
Command Modes	Interface configuration						
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE 3.3SE</td><td>Cisco IOS XE 3.3SE</td></tr> <tr> <td></td><td>This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE		This command was introduced.
Release	Modification						
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE						
	This command was introduced.						
Usage Guidelines	<p>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.</p> <p>Follow these guidelines when configuring the IGMP throttling action:</p> <ul style="list-style-type: none"> • 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 device 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 device 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:

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

The following example shows how to configure the device 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:

```
Device(config)# interface gigabitethernet2/0/1
Device(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 device stack or on a standalone device. 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	<i>profile number</i> 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 3.3SE	This command was introduced.
Usage Guidelines	<p>When you are in IGMP profile configuration mode, you can create a profile by using these commands:</p> <ul style="list-style-type: none">• 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. <p>When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.</p> <p>You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.</p>	

Example

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

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(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 device or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the device stack or on a standalone device. 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 <i>vlan-id</i> (Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.	
Command Default	IGMP snooping is globally enabled on the device. IGMP snooping is enabled on VLAN interfaces.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.
Usage Guidelines	<p>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.</p> <p>VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.</p>	

Example

The following example shows how to globally enable IGMP snooping:

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

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

```
Device(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 <i>vlan-id</i> (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 3.3SE	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 device to the host or the report packet from the host to the device) 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 device, 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 device is processing more than one leave within an LMQI. In such a scenario, the average leave latency is determined by the $(\text{count} + 0.5) * \text{LMQI}$. 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:

```
Device(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 <i>vlan-id</i>		(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. Ranges are 1—1001 and 1006—4094.
address <i>ip-address</i>		(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 <i>response-time</i>		(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1—25 seconds.
query-interval <i>interval-count</i>		(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 <i>count</i>		Sets the number of TCN queries to be executed during the TCN interval time. The range is 1—10.
interval <i>interval</i>		Sets the TCN query interval time. The range is 1—255.
timer expiry <i>expiry-time</i>		(Optional) Sets the length of time until the IGMP querier expires. The range is 60—300 seconds.
version <i>version</i>		(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 device.
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 3.3SE	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:

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

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

```
Device(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:

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

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

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

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

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

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

```
Device(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 device stack or on a standalone device. 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 3.3SE	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 device 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 device sends the first IGMP report from all the hosts for a group to all the multicast routers. The device 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 device 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 device 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:

```
Device(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 vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the device stack or on a standalone device. 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 3.3SE	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:

```
Device(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 device stack or on a standalone device. 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	<i>vlan-id</i>	Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.
	<i>ip-address</i>	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
	interface <i>interface-id</i>	Specifies the interface of the member port. The <i>interface-id</i> has these options: <ul style="list-style-type: none"> • <i>fastethernet interface number</i>—A Fast Ethernet IEEE 802.3 interface. • <i>gigabitethernet interface number</i>—A Gigabit Ethernet IEEE 802.3z interface. • <i>tengigabitethernet interface number</i>—A 10-Gigabit Ethernet IEEE 802.3z interface. • <i>port-channel interface number</i>—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 3.3SE	This command was introduced.
Usage Guidelines	<p>VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.</p> <p>The configuration is saved in NVRAM.</p>	

Example

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

```
Device(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 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 3.3SE	This command was introduced.

Usage Guidelines	None This command is unavailable when using the LAN Base image.
-------------------------	--

Example

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

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

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	<div> vrf <i>vrf-name</i> (Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument. </div> <div> list <i>access-list</i> Specifies the <i>access-list</i> 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. </div>				
Command Default	No PIM register filters are configured.				
Command Modes	Global configuration				
Command History	<table> <tr> <th data-bbox="386 972 878 999">Release</th><th data-bbox="967 972 1521 999">Modification</th></tr> <tr> <td data-bbox="386 1029 878 1056">Cisco IOS XE 3.3SE</td><td data-bbox="967 1029 1521 1056">This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p>				

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.

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

ip pim bsr-candidate

To configure the Device 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 <i>vrf-name</i>	(Optional) Configures the Device to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
	<i>interface-id</i>	ID of the interface on the Device 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.
	<i>hash-mask-length</i>	(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.
	<i>priority</i>	(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 Device is not configured to announce itself as a candidate BSR.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	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 Device 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 Devices 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 Device always accept and process BSR messages. There is no command to disable this function.

Cisco Device 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 Device 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:

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

ip pim rp-candidate

To configure the Device 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 Device 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 (MVRP) instance specified for the <i>vrf-name</i> 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 Device 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 3.3SE	This command was introduced.
Usage Guidelines	Use this command to configure the Device to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.	
	This command should be configured on backbone Devices that have good connectivity to all parts of the PIM domain.	
	The IP address associated with the interface specified by <i>interface-id</i> 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 <i>access-list-number</i> 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.

```
Device(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*]

no ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id*

Syntax Description		
vrf <i>vrf-name</i>	(Optional) Uses Auto-RP to configure groups for which the Device will act as a rendezvous point (RP) for the <i>vrf-name</i> argument.	
<i>interface-id</i>	Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.	
scope <i>ttl-value</i>	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 <i>access-list-number</i>	(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 <i>seconds</i>	(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.	

Command Default Auto-RP is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

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.

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:

ip pim send-rp-announce

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


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 {kpbs | infinity} [group-list access-list]
no ip pim {kpbs | infinity} [group-list access-list]
```

Syntax Description	<i>kpbs</i>	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 3.3SE	Cisco IOS XE 3.3SE This command was introduced.

Example

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

```
Device(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 Device.
any	Allows any match type.
query	Allows only a query from the client for a certain Device in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

Release	Modification
Cisco IOS XE 3.3SE	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:

```
Device(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	<i>line</i> Regular expression to match the service type in packets.				
Command Default	None				
Command Modes	Service list configuration				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE 3.3SE</td><td>This command was introduced.</td></tr></table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				
Usage Guidelines	It is not possible to use the match command if you have used the service-list mdns-sd <i>service-list-name</i> 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:

```
Device(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	<i>line</i> Regular expression to match the service instance in packets.
--------------------	--

Command Default	None
-----------------	------

Command Modes	Service list configuration
---------------	----------------------------

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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:

```
Device(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 <i>route-name</i>	(Optional) Specifies the VPN routing or forwarding instance.
	<i>hostname</i> <i>address</i>	(Optional) Domain Name System (DNS) name or IP address of the multicast router or multilayer switch to query. If omitted, the switch queries itself.
	<i>interface-id</i>	(Optional) Interface ID.
Command Default	The command is disabled.	
Command Modes	User EXEC	
	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.
Usage Guidelines	<p>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.</p> <p>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.)</p>	

Example

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

```
Device# 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
-

redistribute mdns-sd

To redistribute services or service announcements across subnets, use the **redistribute mdns-sd** command. To disable redistribution of services or service announcements across subnets, use the **no** form of this command.

redistribute mdns-sd
no redistribute mdns-sd

This command has no arguments or keywords.

Command Default

The redistribution of services or service announcements across subnets is disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

To redistribute service announcements across interfaces, use the **redistribute mdns-sd** command. This command sends out unsolicited announcements received on one interface to all of the other interfaces. The outgoing announcements are filtered as per the out-service policy defined for the interface, or, in absence of a per-interface service policy, based on the global out-service policy.

In the absence of a redistribute option, services can be discovered by querying in a Layer 3 domain that is not local to the service provider.

Example

The following example shows how to redistribute services or service announcements across subnets:

```
Device(config-mdns)# redistribute mdns-sd
```



Note

If redistribution is enabled globally, global configuration is given higher priority than interface configuration.

service-list mdns-sd

To enter mDNS service discovery service-list mode on the device, use the **service-list mdns-sd** command. To exit mDNS service discovery service-list mode, use the **no** form of this command.

service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]
no service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

Syntax Description	<i>service-list-name</i>	Name of the service list.
	permit <i>sequence number</i>	Permits a filter on the service list to be applied to the sequence number.
	deny <i>sequence number</i>	Denies a filter on the service list to be applied to the sequence number.
	query	Associates a query for the service list name.

Command Default Disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines Service filters are modeled around access lists and route maps.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each 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 terminated once the first statement match is found, and an action, permit, or deny that is associated with the statement match is performed. The default action after scanning through the entire list will be to deny.

This command can be used to enter mDNS service discovery service-list mode.

In this mode you can:

- Create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number.

Example

The following example shows how to create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to a sequence number:

```
Device(config)# service-list mdns-sd s11 permit 3
```


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	<i>service-list-query-name service-list-query-periodicity</i> (Optional) Service-list query periodicity.	
Command Default	Disabled.	
Command Modes	mDNS configuration	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	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:

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

service-routing mdns-sd

To enable the mDNS gateway functionality for a device and enter multicast DNS configuration mode, use the **service-routing mdns-sd** command. To restore the default settings and return to global configuration mode, enter the **no** form of this command.

service-routing mdns-sd

no service-routing mdns-sd

This command has no arguments or keywords.

Command Default	Disabled.
------------------------	-----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines	The mDNS gateway functionality can only be enabled or disabled globally, not on a per-interface basis. The service- filter policy and redistribution can be configured globally as well as on a per-interface basis. Any interface-specific configuration overrides the global configuration.
-------------------------	---

Example

The following example shows how to enable the mDNS gateway functionality for a device and enter multicast DNS configuration mode:

```
Device (config) # service-routing mdns-sd
```

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 3.3SE	This command was introduced.

Example

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

```
Device(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 3.3SE	This command was introduced.

Usage Guidelines	The show ip igmp filter command displays information about all filters defined on the device.
-------------------------	--

Example

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

```
Device# 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 <i>vrf-name</i>	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
	<i>profile number</i>	(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 3.3SE	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 device:

```
Device# 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 device:

```
Device# 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 device 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 <i>vlan-id</i>	(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 3.3SE	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:

```
Device# 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 device:

Device# **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 device 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 <i>vlan-id</i>	(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.
<i>ip_address</i>	(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 3.3SE	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 device.

Device# **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 device.

Device# **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:

Device# **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 device 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 <i>vlan-id</i> (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 3.3SE	This command was introduced.
Usage Guidelines	<p>VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.</p> <p>When multicast VLAN registration (MVR) is enabled, the show ip igmp snooping mrouter command displays MVR multicast router information and IGMP snooping information.</p> <p>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.</p>	

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 device:

```
Device# 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 device, 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

Cisco IOS XE 3.3SE

Modification

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 device.

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 device, 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 device querier.

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

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device 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:

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

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

```
Device> show ip igmp snooping querier detail
```

Vlan	IP Address	IGMP Version	Port
1	1.1.1.1	v2	Fa8/0/1

Global IGMP device 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 device 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 pim autorp

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

show ip pim autorp

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

Command Default	Auto RP is enabled by default.
------------------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines	This command displays whether auto-rp is enabled or disabled.
-------------------------	---

Example

The following command output shows that Auto RP is enabled:

```
Device# 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
```

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 bsr-router

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

Command Default	None
------------------------	------

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

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

```
Device# 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 bsr

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

Command Default	None
------------------------	------

Command Modes	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

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

```
Device# 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 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 <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
	Tunnel <i>interface-number</i>	(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 3.3SE	This command was introduced.

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 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:


```
Device# 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 mdns cache

To display mDNS cache information for the device, use the **show mdns cache** command in privileged EXEC mode.

show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*] | **type** *record-type*]

Syntax Description	<p>interface <i>type-number</i> (Optional) Specifies a particular interface type and number for which mDNS cache information is to be displayed.</p> <p>name <i>record-name</i> (Optional) Specifies a particular name for which mDNS cache information is to be displayed.</p> <p>type <i>record-type</i> (Optional) Specifies a particular type for which mDNS cache information is to be displayed.</p>				
Command Default	None				
Command Modes	Privileged EXEC User EXEC				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE 3.3SE</td><td>This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	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.				

Example

The following is an example of output from the **show mdns cache** command without any keywords:

Device# **show mdns cache**

```
[<NAME>] [TYPE] [CLASS] [TTL/Remaining] [Accessed] [If-name] [Mac Address] [RR Record Data]

_airplay._tcp.local PTR IN 4500/4455 0 V1121
b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

CAMPUS APPLE TV1._airplay._tcp.local SRV IN 120/75 2 V1121
b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

CAMPUS-APPLE-TV1.local A IN 120/75 2 V1121
b878.2e33.c7c5 121.1.0.254

CAMPUS APPLE TV1._airplay._tcp.local TXT IN 4500/4455 2 V1121
b878.2e33.c7c5 (162) 'deviceid=B8:78:2E:33:C7:C6'
```

```

'features=0x5a7ffff7''flags=0x4'

'model=AppleT~'~

_ipp._tcp.local PTR IN 4500/4465 2 V12
2894.0fed.447f EPSON XP-400 Series._ipp._tcp.local

EPSON XP-400 Series._ipp._tcp.local SRV IN 120/85 2 V12
2894.0fed.447f EPSONC053AA.local

EPSONC053AA.local A IN 120/85 2 V12
2894.0fed.447f 121.1.0.251

EPSON XP-400 Series._ipp._tcp.local TXT IN 4500/4465 2 V12
2894.0fed.447f (384)'txtvers=1' N XP-400 Series'

'usbFG=EPSON''usb_MDL=XP~'~

_smb._tcp.local PTR IN 4500/4465 2 V12
2894.0fed.447f EPSON XP-400 Series._smb._tcp.local

EPSON XP-400 Series._smb._tcp.local SRV IN 120/85 2 V12
2894.0fed.447f EPSONC053AA.local

EPSON XP-400 Series._smb._tcp.local TXT IN 4500/4465 2 V12
2894.0fed.447f (1)'' R2-Access1#

```

show mdns requests

To display information for outstanding mDNS requests, including record name and record type information, for the device, use the **show mdns requests** command in privileged EXEC mode.

show mdns requests [**detail** | **name** *record-name* | **type** *record-type* [**name** *record-name*]]

Syntax Description

detail	Displays detailed mDNS request information.
name <i>record-name</i>	Displays detailed mDNS request information based on name.
type <i>record-type</i>	Displays detailed mDNS request information based on type.

Command Default

None

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Example

This is an example of output from the **show mdns requests** command without any keywords:

```
Device# show mdns requests
MDNS Outstanding Requests
=====
Request name  : _airplay._tcp.local
Request type  : PTR
Request class : IN
-----
Request name  : *.*
Request type  : PTR
Request class : IN
```

show mdns statistics

To display mDNS statistics for the device, use the **show mdns statistics** command in privileged EXEC mode.

```
show mdns statistics {all | service-list list-name | service-policy {all | interface type-number
}}
```

Syntax Description	all	Displays the service policy, service list, and interface information.
	service-list <i>list-name</i>	Displays the service list information.
	service-policy	Displays the service policy information.
	interface <i>type number</i>	Displays interface information.
Command Default	None	
Command Modes	Privileged EXEC	
	User EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	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.	

Example

The following is a sample output from the **show mdns statistics all** command:

```
Device# show mdns statistics all

mDNS Statistics
mDNS packets sent      : 0
mDNS packets received  : 0
mDNS packets dropped    : 0
mDNS cache memory in use: 64224(bytes)
```

show platform software fed switch ip multicast

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

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

Syntax Description	switch { <i>switch_num</i> active standby }	The device for which you want to display information. <ul style="list-style-type: none"> • <i>switch_num</i>—Enter the switch ID. Displays information for the specified switch. • active—Displays information for the active switch. • standby—Displays information for the standby switch, if available.
	groups	Displays the IP multicast routes per group.
	hardware [detail]	Displays the IP multicast routes loaded into hardware. The optional detail keyword is used to show the port members in the destination index and route index.
	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 Everest 16.5.1a	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:

```
Device# 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

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

=====

```
show platform software fed switch ip multicast
```

```
<output truncated>
```