IP Multicast Commands

cache-memory-max

To set a percentage of the system memory for cache, use the **cache-memory-max** command. To remove a 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

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. The memory is set by default to a maximum of 10 percent of the system memory.

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.

Examples

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

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

clear ip mfib counters

To clear all active IPV4 multicast forwarding information base (MFIB) traffic counters, use the **clear ip mfib counters** privileged exec command.

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

Syntax Description

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

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

None

Examples

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

```
Switch# clear ip mfib counters
```

The following example shows how to reset the IP multicast forwarding information base cache counters to the global default configuration:

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

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

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

clear ip mroute

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

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 3.3SECisco 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.

Examples

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

```
Switch# clear ip mroute *
```

The following example shows how to delete all 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:

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

ip igmp filter

To control whether or not all 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 switch stack or on a standalone switch. 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	The IGMP profile number to be applied. The range is 1 to 4294967295.

Command Default

No IGMP filters are applied.

Command Modes

Interface configuration

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 switch port interfaces, but one port can have only one profile applied to it.

Examples

You can verify your setting by using the **show running-config** privileged EXEC command 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 switch stack or on a standalone switch. 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	The maximum number of IGMP groups that an interface can join. The range is 0 to 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 switch 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 3.3SECisco IOS XE 3.3SE	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 limitation, 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 switch 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 switch 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.

Examples

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

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

This example shows how to configure the switch 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:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(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 switch stack or on a standalone switch. 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 to 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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create the 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.

Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

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

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

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the switch stack or on a standalone switch. 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. The range is 1 to 1001 and 1006 to 4094.

Command Default

IGMP snooping is globally enabled on the switch.

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

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.

Examples

This example shows how to globally enable IGMP snooping:

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

This example shows how to enable IGMP snooping on VLAN 1:

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

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

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 the 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 to 1001. Do not enter leading zeroes.
count	The interval at which query messages are sent, in milliseconds. The range is from 1 to 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 3.3SECisco 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 to the last-member queries are received 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 switch to the host or the report packet from the host to the switch) may result in traffic forwarding being stopped even if there is still a receiver. Traffic continues to be forwarded after the next general query is sent by the switch, 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 one last-member-query-interval (LMQI) value when the switch is processing more than one leave within an LMQI. In this case, 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.

Examples

The following example sets the last member query count to 5:

```
Switch(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. The range is 1 to 1001 and 1006 to 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 to 25 seconds.
query-interval *interval-count*	(Optional) Sets the interval between IGMP queriers. The range is 1 to 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 to 10.
interval *interval*	Sets the TCN query interval time. The range is 1 to 255.
timer expiry *expiry-time*	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version *version*	(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.

Command Default

The IGMP snooping querier feature is globally disabled on the switch.

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 3.3SECisco 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 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

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

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

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

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

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

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

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

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

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

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

This example shows how to set the IGMP snooping querier feature to version 2:

```
Switch(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 switch stack or on a standalone switch. 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 3.3SECisco 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 switch 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 switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch 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 switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch 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.

Examples

This example shows how to disable report suppression:

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

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

ip igmp snooping vlan mrouter

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

Examples This example shows how to configure a port as a multicast router port:

```
Switch(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 switch stack or on a standalone switch. Use the **no** form of this command to remove ports specified as members of a static multicast group.

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. The range is 1 to 1001 and 1006 to 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* value 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 to 128.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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.

Examples

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

```
Switch(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** privileged EXEC command.

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 the 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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to enable authentication, authorization, and accounting (AAA) on IP multicast:

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

ip multicast vlan

To configure IP multicast on a single VLAN, use the **ip multicast vlan** command in global configuration mode. To remove the VLAN from the WLAN, use the **no** form of the command.

ip multicast vlan {*vlan-name* | *vlan-id*}

no ip multicast vlan{*vlan-name* | *vlan-id*}

Syntax Description

vlan-name	Specifies the VLAN name.
vlan-id	Specifies the VLAN ID.

Command Default

Disabled.

Command Modes

WLAN configuration

Command History

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

Usage Guidelines

None

Examples

This example configures vlan_id01 as a multicast VLAN.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan 1
Switch(config-wlan)# ip multicast vlan vlan_id01
```

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 to 199 and an expanded range of 2000 to 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 3.3SECisco IOS XE 3.3SE	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 filter on 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 desired, use the **ip multicast boundary** command instead.

Examples

The following example shows how to permit register packets for any 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.

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

ip pim bsr-candidate

To configure the switch 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 switch 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 this switch 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 switch is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SECisco 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 switch 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 switches 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 preexisting 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 switches always accept and process BSR messages. There is no command to disable this function.

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

- A longest match lookup is performed on the group prefix that is announced by the BSR C-RPs.
- If more than one BSR-learned C-RP are 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 have the same priority, the BSR hash function is used to select the RP for a group.
- If more than one BSR-learned C-RP return the same hash value derived from the BSR hash function, the BSR C-RP with the highest IP address is preferred.

Examples

The following example shows how to configure the IP address of the switch 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:

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

ip pim rp-candidate

To configure the switch 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 this switch 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 switch 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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

This command should be configured on backbone switches 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.

Examples

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.

```
Switch(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 switch will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this switch 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 *vrf-name*	(Optional) Uses Auto-RP to configure groups for which the switch 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 so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 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 to 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 holdtime 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 to 16383.

Command Default

Auto-RP is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Enter this command on the switch 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.

Examples

The following example shows how to configure the switch 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:

```
Switch(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 {*kbps* | **infinity**} [**group-list** *access-list*]

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

Syntax Description

kbps	The 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 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 groups.

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Examples

The following example makes all sources for access list 16 use the shared tree:

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

match message-type

To set the message type to match for 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, each one has a permit or deny result. Evaluation of 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 an action permit/deny 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.

Examples

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

```
Switch(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 service type 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.

Examples

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

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

match service-instance

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

match servcie-instance *line*

Syntax Description

line	Regular expression to match 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.

Examples

This example shows how to set the service instance to match:

```
Switch(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) The 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) Specifies the interface ID.

Command Default

The command is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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 have supported responding to mrinfo requests since 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.)

Examples

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

```
Switch# 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 (SNMP)-capable
- A: Auto-Rendezvous Point (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.

Examples

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

```
Switch(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 switch, use the **service-list mdns-sd** command. To exit mDNS service discovery service-list mode, use the **no** form of the 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

service-list-name	Name of the service list.
permit *sequence number*	Permits a filter on the service list to be applied to the sequence number.
deny *sequence number*	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 will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each has a permit or deny result. 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 aborted once the first statement match is found and an action, permit or deny associated with the statement match is performed. 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.

Examples

This 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 the sequence number:

```
Switch(config)# service-list mdns-sd sl1 permit 3
```

service-policy-query

To configure 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) Configures the 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

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

Examples

This example shows how to configure service list query periodicity:

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

service-routing mdns-sd

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

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.

Examples

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

```
Switch(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 the command.

service-policy *service-policy-name* {**IN** | **OUT**}

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

Syntax Description

service-policy-name **IN**	Applies a filter on incoming service discovery information.
service-policy-name **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.

Usage Guidelines

The Switch intercepts mDNS packets. If they are mDNS messages destined to a wireless client (for example, the destination MAC is client's MAC address), and the client's mobility state is either local or foreign, the destination MAC address is overwritten with the client's MAC address and enqueues the packet to be sent out on the associated CAPWAP tunnel.

Examples

This example applies a filter on incoming service discovery information on a service list:

```
Switch(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 command 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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# show ip igmp filter

IGMP filter enabled
```

show ip igmp profile

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

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) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.

Command Default

IGMP profiles undefined by default.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

None

Examples

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

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

This example shows the output of the **show ip igmp profile** privileged EXEC command for all profiles configured on the switch:

```
Switch# 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 switch or the VLAN, use the **show ip igmp snooping** command in user or privileged EXEC command 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 3.3SECisco IOS XE 3.3SE	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.

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

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Switch# 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
```

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch:

```
Switch# 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
<output truncated>
```

show ip igmp snooping groups

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

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 3.3SECisco 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

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch:

```
Switch# 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
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch:

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of 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:

```
Switch# 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 igmpv2-tracking

To display group and IP address entries, use the **show ip igmp snooping igmpv2-tracking** command in privileged EXEC mode.

Note The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

show ip igmp snooping igmpv2-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

show ip igmp snooping mrouter

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

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

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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.

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.

Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch:

```
Switch# 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 configured on a switch, use the **show ip igmp snooping querier** user EXEC command.

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

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays detailed IGMP querier information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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 has 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 switch.

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 switch, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier is learned 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 switch querier.

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

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

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> 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
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail
Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP switch 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 switch 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 igmp snooping wireless mcast-spi-count

To display the statistics of the number of multicast stateful packet inspections (SPIs) per multicast group ID (MGID) sent to the switch, use the **show ip igmp snooping wireless mcast-spi-count** command in privileged EXEC mode.

show ip igmp snooping wireless mcast-spi-count

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

None

Examples

This is an example of output from the **show ip igmp snooping wireless mcast-spi-count** command:

```
Switch# show ip igmp snooping wireless mcast-spi-count

Stats for Mcast Client Add/Delete SPI Messages Sent to WCM

MGID    ADD MSGs        Del MSGs
--------------------------------
4160    1323            667
```

show ip igmp snooping wireless mgid

To display multicast group ID (MGID) mappings, use the **show ip igmp snooping wireless mgid** command in privileged EXEC mode.

show ip igmp snooping wireless mgid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

None

Examples

This is an example of output from the **show ip igmp snooping wireless mgid** command:

```
Switch# show ip igmp snooping wireless mgid

Total number of L2-MGIDs    = 0

Total number of MCAST MGIDs = 0

 Wireless multicast is Enabled in the system
 Vlan     bcast   nonip-mcast   mcast    mgid    Stdby Flags
 1      Disabled   Disabled   Enabled    Disabled  0:0:1:0
 25     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 34     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 200    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 1002   Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1003   Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1004   Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1005   Enabled    Enabled    Enabled    Disabled  0:0:1:0

Index  MGID                 (S, G, V)
-----------------------------------------------------------
```

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 mode

Command History

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

Usage Guidelines

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

Examples

The following command output displays that auto-rp is enabled:

```
Switch# 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 3.3SECisco 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 will display the BSR router information.

Examples

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

```
Switch# 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 3.3SECisco 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 will display the BSR router information.

Examples

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

```
Switch# 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 *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
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 3.3SECisco 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
```

Examples

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:

```
Switch# 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 switch, use the **show mdns cache** privileged EXEC command.

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

Syntax Description

interface *type-number*	(Optional) Specifies a particular interface type and number for which mDNS cache information is to be displayed.
name *record-name*	(Optional) Specifies a particular name for which mDNS cache information is to be displayed.
type *record-type*	(Optional) Specifies a particular type for which mDNS cache information is to be displayed.

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.

Examples

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

```
Switch# show mdns cache
```

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

_airplay._tcp.local                   PTR     IN      4500/4455         0        Vl1121
b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

CAMPUS APPLE TV1._airplay._tcp.local SRV     IN      120/75            2        Vl1121
b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

CAMPUS-APPLE-TV1.local                A       IN      120/75            2        Vl1121
b878.2e33.c7c5  121.1.0.254

CAMPUS APPLE TV1._airplay._tcp.local TXT     IN      4500/4455         2        Vl1121
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        Vl2
2894.0fed.447f  EPSON XP-400 Series._ipp._tcp.local

EPSON XP-400 Series._ipp._tcp.local  SRV     IN      120/85            2        Vl2
2894.0fed.447f  EPSONC053AA.local

EPSONC053AA.local                     A       IN      120/85            2        Vl2
2894.0fed.447f  121.1.0.251

EPSON XP-400 Series._ipp._tcp.local  TXT     IN      4500/4465         2        Vl2
2894.0fed.447f  (384)'txtvers=1' N XP-400 Series'

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

_smb._tcp.local                       PTR     IN      4500/4465         2        Vl2
2894.0fed.447f  EPSON XP-400 Series._smb._tcp.local

EPSON XP-400 Series._smb._tcp.local  SRV     IN      120/85            2        Vl2
2894.0fed.447f  EPSONC053AA.local

EPSON XP-400 Series._smb._tcp.local  TXT     IN      4500/4465         2        Vl2
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 switch, use the **show mdns requests** privileged EXEC command.

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

Syntax Description

detail	Displays detailed mDNS requests information.
name *record-name*	Displays detailed mDNS requests information based on name.
type *record-type*	Displays detailed mDNS requests 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.

Examples

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

```
Switch# 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 switch, use the **show mdns statistics** privileged EXEC command.

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 *list-name*	Displays the service list information.
service-policy	Displays the service policy information.
interface *type number*	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.

Examples

This is an example of output from the **show mdns statistics all** command:

```
Switch# 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 ip multicast

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

show platform ip multicast {**groups** | **hardware [detail]** | **interfaces** | **retry**}

Syntax Description

groups	Displays IP multicast routes per group.
hardware [**detail**]	Displays IP multicast routes loaded into hardware. The optional **detail** keyword is used to show port members in the destination index and route index.
interfaces	Displays IP multicast interfaces.
retry	Displays the IP multicast routes in the retry queue.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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.

Examples

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

```
Switch# show platform 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

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

RI details
----------

SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f6
RM:fd const lbl = 0x0
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1
```

```
============================================================

HTM details
-----------
Handle:0x5d604490 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x5d604518  handle1:0x5d604580


Detailed Resource Information (ASIC# 0)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x5d604518)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x5d604580)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0

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


MROUTE ENTRY vrf 0 (*, 224.0.1.40)
Token: 0x0000001f8  flags:  C IC
RPF interface: Vl121(74238750229529173)): SVI
Token:0x00000021  flags: F IC NS
Number of OIF: 1
Flags: 0x10   Pkts : 0
OIF Details:
     Vl121      F IC NS
DI details
----------
Handle:0x603d0000 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: index0:0x51f7  index1:0x51f7

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xe0 0x0 0x1 0x28 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 = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
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 = 0x51f7
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 = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
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 = 0x51f7
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

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

RI details
----------

SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f7
RM:fd const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x1
RM:remote data = 0x1

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

HTM details
-----------
Handle:0x603d0440 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x603cfae0  sm handle 0:0x603d0590  handle1:0x603d0520
sm handle 1:0x603d1770


Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x603cfae0)
```

```
KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x603d0520)

KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0

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


MROUTE ENTRY vrf 0 (*, 239.255.255.250)
Token: 0x0000003b7d  flags:  C
No RPF interface.
Number of OIF: 1
Flags: 0x10   Pkts : 95
OIF Details:
     Vl131      F NS
DI details
----------
Handle:0x606ffba0 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: index0:0x51f8  index1:0x51f8

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xef 0xff 0xff 0xfa 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 = 0x51f8
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 = 0x51f8
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 = 0x51f8
RM:pmap = 0x0
```

```
RM:cmi = 0x0
RM:rcp_pmap = 0x1
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 = 0x51f8
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

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

RI details
----------

ASIC# 0
Replication list :
------------------

Total #ri : 0
start_ri : 15
common_ret : 0


ASIC# 1
Replication list :
------------------

Total #ri : 6
start_ri : 15
common_ret : 0

Replication entry rep_ri 0xF #elem = 1
0) ri[0]=50 port=58 dirty=0


ASIC# 2
Replication list :
------------------

Total #ri : 0
start_ri : 0
common_ret : 0


SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f8
RM:fd const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1

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

HTM details
-----------
```

```
Handle:0x606ff6f8 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x606ff3e0  sm handle 0:0x60ab9160  handle1:0x606ff378
sm handle 1:0x60ab6cc0


Detailed Resource Information (ASIC# 0)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x606ff3e0)

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x606ff378)

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0

============================================================
```

wireless mdns-bridging

To enable Ethernet mDNS support, use the **wireless mdns-bridging** command. To disable Ethernet mDNS support, use the **no** form of this command.

wireless mdns-bridging

no wireless mdns-bridging

This command has no keywords or arguments.

Command Default

Ethernet mDNS support is enabled by default.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command only if you have enabled wireless multicast.

Examples

This example shows how to enable Ethernet mDNS support:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wireless mdns-bridging
```

wireless multicast

To enable Ethernet multicast support, use the **wireless multicast** command.

wireless multicast [**non-ip** [**vlan** *vlan-id*]]

Syntax Description

non-ip	(Optional) Configures multicast non-IP support.
vlan *vlan-id*	(Optional) Specifies multicast non-IP for a VLAN. The interface number ranges between 1 and 4095.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

None

Examples

This example shows how to configure multicast non-IP VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast non-ip vlan 20
```