



IP Multicast Commands

- [cache-memory-max](#), page 3
- [ip igmp filter](#), page 4
- [ip igmp max-groups](#), page 5
- [ip igmp profile](#), page 7
- [ip igmp snooping](#), page 9
- [ip igmp snooping last-member-query-count](#), page 10
- [ip igmp snooping querier](#), page 12
- [ip igmp snooping report-suppression](#), page 14
- [ip igmp snooping vlan mrouter](#), page 16
- [ip igmp snooping vlan static](#), page 17
- [ip multicast vlan](#), page 19
- [match message-type](#), page 20
- [match service-instance](#), page 21
- [match service-type](#), page 22
- [service-list mdns-sd](#), page 23
- [service-routing mdns-sd](#), page 25
- [service-policy](#), page 26
- [redistribute mdns-sd](#), page 27
- [service-policy-query](#), page 28
- [show ip igmp filter](#), page 29
- [show ip igmp profile](#), page 30
- [show ip igmp snooping](#), page 31
- [show ip igmp snooping groups](#), page 33
- [show ip igmp snooping igmpv2-tracking](#), page 35

- [show ip igmp snooping mrouter](#), page 36
- [show ip igmp snooping querier](#), page 37
- [show ip igmp snooping wireless mcast-spi-count](#), page 39
- [show ip igmp snooping wireless mgid](#), page 40
- [show mdns cache](#), page 41
- [show mdns requests](#), page 43
- [show mdns statistics](#), page 44
- [show wireless multicast](#), page 45
- [show wireless multicast group](#), page 46
- [wireless multicast](#), page 47
- [wireless mdns-bridging](#), page 48

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

Cisco IOS XE 3.3SE

Modification

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:

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

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 controller stack or on a standalone controller. 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	<i>profile number</i>	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 3.2SE	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 controller 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.

Related Commands	Command	Description
	ip igmp profile	Configures and enters IGMP Filter Profile configuration mode.
	show ip dhcp snooping statistics	Displays DHCP snooping statistics.

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 controller stack or on a standalone controller. 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

<i>max number</i>	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 controller 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 3.2SE	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 controller 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 controller 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:

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

This example shows how to configure the controller 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:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(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 controller stack or on a standalone controller. 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 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 3.2SE	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:

```
Controller(config)# ip igmp profile 40
Controller(config-igmp-profile)# permit
Controller(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.

Related Commands

Command	Description
ip igmp filter	Applies IGMP profile to the interface.
show ip igmp profile	Displays configured IGMP profiles specified by the command.

ip igmp snooping

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

Command Default

IGMP snooping is globally enabled on the controller.
IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	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:

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

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

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

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

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.

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 <i>vlan-id</i>	(Optional) Sets the count value on a specific VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
<i>count</i>	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 3.2SE	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 controller to the host or the report packet from the host to the controller) 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 controller, 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 controller is processing more than one leave within an LMQI. In this case, 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.

Examples

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

```
Controller(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. The range is 1 to 1001 and 1006 to 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 to 25 seconds.
query-interval <i>interval-count</i>	(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 <i>count</i>	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.
interval <i>interval</i>	Sets the TCN query interval time. The range is 1 to 255.
timer expiry <i>expiry-time</i>	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version <i>version</i>	(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 controller.

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 3.2SE	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:

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.

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 controller stack or on a standalone controller. 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 3.2SE	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 controller 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 controller sends the first IGMP report from all hosts for a group to all the multicast routers. The controller 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 controller 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 controller 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:

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

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

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping configurations.

ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the controller stack or on a standalone controller. 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 3.2SE	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:

```
Controller(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.

Related Commands	Command	Description
	ip igmp snooping report-suppression	Enables IGMP report suppression.
	show ip igmp snooping	Displays IGMP snooping configurations.
	show ip igmp snooping groups	Displays the IGMP snooping multicast table.
	show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
	show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

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 controller stack or on a standalone controller. 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

<i>vlan-id</i>	Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 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> value 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 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 3.2SE	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:

```
Controller(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.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

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

<i>vlan-name</i>	Specifies the VLAN name.
<i>vlan-id</i>	Specifies the VLAN ID.

Command Default

Disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example configures `vlan_id01` as a multicast VLAN.

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

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:

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

match service-instance

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

match service-instance *line*

Syntax Description	<i>line</i>	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:

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

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 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:

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

service-list mdns-sd

To enter mDNS service discovery service-list mode on the controller, 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

<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 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:

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


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:

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

Related Commands

Command	Description
match message-type	Sets the message type to match.
match service-instance	Sets the service instance to match.
match service-type	Sets the value of the mDNS service type string to match.

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

<i>service-policy-name</i> IN	Applies a filter on incoming service discovery information.
--------------------------------------	---

<i>service-policy-name</i> 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 Controller 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:

```
Controller(config-mdns)# service-policy serv-poll IN
```

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:

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



Note

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

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:

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

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 <i>vrf-name</i>	(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 3.2SE	This command was introduced.

Usage Guidelines

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

Examples

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

```
Controller# 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

<i>vrf vrf-name</i>	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
<i>profile number</i>	(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 3.2SE	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 controller:

```
Controller# 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 controller:

```
Controller# 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
```

Related Commands

Command	Description
ip igmp profile	Configures and enters IGMP Filter Profile configuration mode.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the controller 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 <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 3.2SE	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:

```
Controller# 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
```

show ip igmp snooping

```
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 controller:

```
Controller# 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>
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the controller 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 <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 3.2SE	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 controller:

```
Controller# show ip igmp snooping groups
Vlan      Group          Type          Version      Port List
-----
1         224.1.4.4      igmp
1         224.1.4.5      igmp
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 controller:

```
Controller# 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:

```
Controller# 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
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping	Displays IGMP snooping configurations.

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 3.2SE	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 controller 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 3.2SE	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 controller:

```
Controller# show ip igmp snooping mrouter
Vlan      ports
----      -
  1       Gi2/0/1 (dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.

show ip igmp snooping querier

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

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

Syntax Description

vlan <i>vlan-id</i>	(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 3.2SE	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 controller.

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 controller, 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 controller querier.

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

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

```
Controller> 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:

```
Controller> show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1        v2                 Fa8/0/1
Global IGMP controller 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 controller 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
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping querier	Globally enables the IGMP querier function.
show ip igmp snooping	Displays IGMP snooping configurations.

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 controller, 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 3.2SE	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:

```
Controller# 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 3.2SE	This command was introduced.

Usage Guidelines None

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

```

Controller# 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 mdns cache

To display mDNS cache information for the controller, 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 <i>type-number</i>	(Optional) Specifies a particular interface type and number for which mDNS cache information is to be displayed.
name <i>record-name</i>	(Optional) Specifies a particular name for which mDNS cache information is to be displayed.
type <i>record-type</i>	(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:

```
Controller# 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 (I62) 'deviceid=B8:78:2E:33:C7:C6'
```

show mdns cache

```

      '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 controller, 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 <i>record-name</i>		Displays detailed mDNS requests information based on name.
type <i>record-type</i>		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:

```
Controller# 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 controller, 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 <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.

Examples

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

```
Controller# 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 wireless multicast

To display wireless multicast information, use the **show wireless multicast** command in privileged EXEC mode.

show wireless multicast [**source** *source-ip* **group** *group-ip* **vlan** *vlan-id* | **group** *group-ip* **vlan** *vlan-id*]

Syntax Description		
source <i>source-ip</i>	(Optional) Specifies the source IPv4 and IPv6 address of multicast traffic.	
group <i>group-ip</i>	(Optional) Specifies the destination group and group IP of multicast traffic.	
vlan <i>vlan-id</i>	Displays the client information on VLAN with the specific VLAN ID.	

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines None

Examples This example shows how to display the wireless multicast information:

```

Controller# show wireless multicast

Multicast                               : Enabled
AP Capwap Multicast                     : Unicast
Wireless Broadcast                       : Disabled
Wireless Multicast non-ip-mcast         : Disabled

Vlan      Non-ip-mcast      Broadcast      MGID
-----
1          Enabled         Enabled        Enabled
2          Enabled         Enabled        Disabled
94         Enabled         Enabled        Disabled

```

show wireless multicast group

To display the information of the wireless-multicast non-ip VLANs or the group, use the **show wireless multicast group** command in privileged EXEC mode.

show wireless multicast group {**summary** | *group-ip* **vlan** *vlan-id*}

Syntax Description

summary	Displays wireless-multicast non-ip group summary.
<i>group-ip</i>	Specifies the group IP address.
vlan <i>vlan-id</i>	Specifies the destination group IPv4/IPv6 Address of multicast traffic.

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the wireless-multicast non-ip group summary.

```
Controller# show wireless multicast group summary
```

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 <i>vlan-id</i>	(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 3.2SE	This command was introduced.

Usage Guidelines None

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

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

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:

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