



# CHAPTER 18

## Configuring IGMP Snooping

---

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 2960 switch. It also includes procedures for controlling multicast group membership by using IGMP filtering and procedures for configuring the IGMP throttling action.

**Note**

---

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the “IP Multicast Routing Commands” section in the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*.

---

This chapter consists of these sections:

- [Understanding IGMP Snooping, page 18-1](#)
- [Configuring IGMP Snooping, page 18-6](#)
- [Displaying IGMP Snooping Information, page 18-14](#)
- [Configuring IGMP Filtering and Throttling, page 18-16](#)
- [Displaying IGMP Filtering and Throttling Configuration, page 18-21](#)

**Note**

---

You can either manage IP multicast group addresses through features such as IGMP snooping, or you can use static IP addresses.

---

## Understanding IGMP Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

**Note**

---

For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.

---

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the **ip igmp snooping vlan *vlan-id* static *ip\_address* interface *interface-id*** global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed. For more information about the IGMP snooping querier, see the “[Configuring the IGMP Snooping Querier](#)” section on page 18-13.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

- [IGMP Versions, page 18-2](#)
- [Joining a Multicast Group, page 18-3](#)
- [Leaving a Multicast Group, page 18-4](#)
- [Immediate Leave, page 18-5](#)
- [IGMP Configurable-Leave Timer, page 18-5](#)
- [IGMP Report Suppression, page 18-5](#)

## IGMP Versions

The switch supports IGMP Version 1, IGMP Version 2, and IGMP Version 3. These versions are interoperable on the switch. For example, if IGMP snooping is enabled on an IGMPv2 switch and the switch receives an IGMPv3 report from a host, the switch can forward the IGMPv3 report to the multicast router.



### Note

The switch supports IGMPv3 snooping based only on the destination multicast MAC address. It does not support snooping based on the source MAC address or on proxy reports.

An IGMPv3 switch supports Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when your network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv2 or IGMPv1 hosts.



### Note

IGMPv3 join and leave messages are not supported on switches running IGMP filtering.

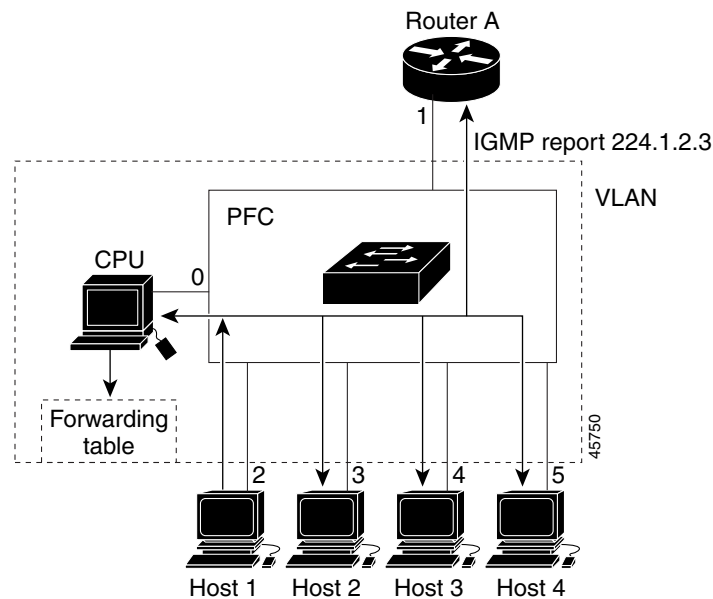
An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature. For more information about source-specific multicast with IGMPv3 and IGMP, see the following URL:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products\\_feature\\_guide09186a008008048a.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008048a.html)

## Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group and it is an IGMP Version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP Version 1 or Version 2 hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group. See [Figure 18-1](#).

**Figure 18-1** Initial IGMP Join Message



Router A sends a general query to the switch, which forwards the query to ports 2 through 5, which are all members of the same VLAN. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. The switch CPU uses the information in the IGMP report to set up a forwarding-table entry, as shown in [Table 18-1](#), that includes the port numbers connected to Host 1 and the router.

**Table 18-1** IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2



## Immediate Leave

Immediate Leave is only supported on IGMP Version 2 hosts.

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

**Note**

You should only use the Immediate Leave feature on VLANs where a single host is connected to each port. If Immediate Leave is enabled in VLANs where more than one host is connected to a port, some hosts might inadvertently be dropped.

For configuration steps, see the [“Enabling IGMP Immediate Leave” section on page 18-9](#).

## IGMP Configurable-Leave Timer

You can configure the time that the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 5000 milliseconds. The timer can be set either globally or on a per-VLAN basis. The VLAN configuration of the leave time overrides the global configuration.

For configuration steps, see the [“Configuring the IGMP Leave Timer” section on page 18-10](#).

## IGMP Report Suppression

**Note**

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 router 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 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, all IGMP reports are forwarded to the multicast routers. For configuration steps, see the [“Disabling IGMP Report Suppression” section on page 18-14](#).

# Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. These sections contain this configuration information:

- [Default IGMP Snooping Configuration, page 18-6](#)
- [Enabling or Disabling IGMP Snooping, page 18-6](#)
- [Setting the Snooping Method, page 18-7](#)
- [Configuring a Multicast Router Port, page 18-8](#)
- [Configuring a Host Statically to Join a Group, page 18-9](#)
- [Enabling IGMP Immediate Leave, page 18-9](#)
- [Configuring the IGMP Leave Timer, page 18-10](#)
- [Configuring TCN-Related Commands, page 18-11](#)
- [Configuring the IGMP Snooping Querier, page 18-13](#)
- [Disabling IGMP Report Suppression, page 18-14](#)

## Default IGMP Snooping Configuration

[Table 18-3](#) shows the default IGMP snooping configuration.

**Table 18-3** Default IGMP Snooping Configuration

Feature	Default Setting
IGMP snooping	Enabled globally and per VLAN
Multicast routers	None configured
Multicast router learning (snooping) method	PIM-DVMRP
IGMP snooping Immediate Leave	Disabled
Static groups	None configured
TCN <sup>1</sup> flood query count	2
TCN query solicitation	Disabled
IGMP snooping querier	Disabled
IGMP report suppression	Enabled

1. TCN = Topology Change Notification

## Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the switch. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. IGMP snooping is by default enabled on all VLANs, but can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the VLAN IGMP snooping. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable VLAN snooping.

Beginning in privileged EXEC mode, follow these steps to globally enable IGMP snooping on the switch:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping</b>	Globally enable IGMP snooping in all existing VLAN interfaces.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To globally disable IGMP snooping on all VLAN interfaces, use the **no ip igmp snooping** global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN interface:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping vlan <i>vlan-id</i></b>	Enable IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094.  <b>Note</b> IGMP snooping must be globally enabled before you can enable VLAN snooping.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable IGMP snooping on a VLAN interface, use the **no ip igmp snooping vlan *vlan-id*** global configuration command for the specified VLAN number.

## Setting the Snooping Method

Multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns of such ports through one of these methods:

- Snooping on IGMP queries, Protocol Independent Multicast (PIM) packets, and Distance Vector Multicast Routing Protocol (DVMRP) packets
- Listening to Cisco Group Management Protocol (CGMP) packets from other routers
- Statically connecting to a multicast router port with the **ip igmp snooping mrouter** global configuration command

You can configure the switch either to snoop on IGMP queries and PIM/DVMRP packets or to listen to CGMP self-join or proxy-join packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through only CGMP packets, use the **ip igmp snooping vlan *vlan-id* mrouter learn cgmp** global configuration command. When this command is entered, the router listens to only CGMP self-join and CGMP proxy-join packets and to no other CGMP packets. To learn of multicast router ports through only PIM-DVMRP packets, use the **ip igmp snooping vlan *vlan-id* mrouter learn pim-dvmrp** global configuration command.

**Note**

If you want to use CGMP as the learning method and no multicast routers in the VLAN are CGMP proxy-enabled, you must enter the **ip cgmp router-only** command to dynamically access the router.

Beginning in privileged EXEC mode, follow these steps to alter the method in which a VLAN interface dynamically accesses a multicast router:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp   pim-dvmrp}</b>	Enable IGMP snooping on a VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.  Specify the multicast router learning method: <ul style="list-style-type: none"> <li>• <b>cgmp</b>—Listen for CGMP packets. This method is useful for reducing control traffic.</li> <li>• <b>pim-dvmrp</b>—Snoop on IGMP queries and PIM-DVMRP packets. This is the default.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show ip igmp snooping</b>	Verify the configuration.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default learning method, use the **no ip igmp snooping vlan *vlan-id* mrouter learn cgmp** global configuration command.

This example shows how to configure IGMP snooping to use CGMP packets as the learning method:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

## Configuring a Multicast Router Port

To add a multicast router port (add a static connection to a multicast router), use the **ip igmp snooping vlan mrouter** global configuration command on the switch.

Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i></b>	Specify the multicast router VLAN ID and the interface to the multicast router. <ul style="list-style-type: none"> <li>• The VLAN ID range is 1 to 1001 and 1006 to 4094.</li> <li>• The interface can be a physical interface or a port channel. The port-channel range is 1 to 6.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.

	Command	Purpose
Step 4	<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	Verify that IGMP snooping is enabled on the VLAN interface.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove a multicast router port from the VLAN, use the **no ip igmp snooping vlan *vlan-id* mrouter interface *interface-id*** global configuration command.

This example shows how to enable a static connection to a multicast router:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# end
```

## Configuring a Host Statically to Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip igmp snooping vlan <i>vlan-id</i> static <i>ip_address</i> interface <i>interface-id</i></code>	Statically configure a Layer 2 port as a member of a multicast group: <ul style="list-style-type: none"> <li>• <i>vlan-id</i> is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094.</li> <li>• <i>ip-address</i> is the group IP address.</li> <li>• <i>interface-id</i> is the member port. It can be a physical interface or a port channel (1 to 6).</li> </ul>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show ip igmp snooping groups</code>	Verify the member port and the IP address.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove the Layer 2 port from the multicast group, use the **no ip igmp snooping vlan *vlan-id* static *mac-address* interface *interface-id*** global configuration command.

This example shows how to statically configure a host on a port:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet0/1
Switch(config)# end
```

## Enabling IGMP Immediate Leave

When you enable IGMP Immediate Leave, the switch immediately removes a port when it detects an IGMP Version 2 leave message on that port. You should only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN.



**Note** Immediate Leave is supported only on IGMP Version 2 hosts.

Beginning in privileged EXEC mode, follow these steps to enable IGMP Immediate Leave:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip igmp snooping vlan <i>vlan-id</i> immediate-leave</code>	Enable IGMP Immediate Leave on the VLAN interface.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show ip igmp snooping vlan <i>vlan-id</i></code>	Verify that Immediate Leave is enabled on the VLAN interface.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To disable IGMP Immediate Leave on a VLAN, use the **no ip igmp snooping vlan *vlan-id* immediate-leave** global configuration command.

This example shows how to enable IGMP Immediate Leave on VLAN 130:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

## Configuring the IGMP Leave Timer

Follows these guidelines when configuring the IGMP leave timer:

- You can configure the leave time globally or on a per-VLAN basis.
- Configuring the leave time on a VLAN overrides the global setting.
- The default leave time is 1000 milliseconds.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2.
- The actual leave latency in the network is usually the configured leave time. However, the leave time *might* vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

Beginning in privileged EXEC mode, follow these steps to enable the IGMP configurable-leave timer:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip igmp snooping last-member-query-interval <i>time</i></code>	Configure the IGMP leave timer globally. The range is 100 to 5000 milliseconds. The default is 1000 seconds.
Step 3	<code>ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval <i>time</i></code>	(Optional) Configure the IGMP leave time on the VLAN interface. The range is 100 to 5000 milliseconds. <b>Note</b> Configuring the leave time on a VLAN overrides the globally configured timer.
Step 4	<code>end</code>	Return to privileged EXEC mode.

	Command	Purpose
Step 5	<b>show ip igmp snooping</b>	(Optional) Display the configured IGMP leave time.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To globally reset the IGMP leave timer to the default setting, use the **no ip igmp snooping last-member-query-interval** global configuration command.

To remove the configured IGMP leave-time setting from the specified VLAN, use the **no ip igmp snooping vlan *vlan-id* last-member-query-interval** global configuration command.

## Configuring TCN-Related Commands

These sections describe how to control flooded multicast traffic during a TCN event:

- [Controlling the Multicast Flooding Time After a TCN Event, page 18-11](#)
- [Recovering from Flood Mode, page 18-12](#)
- [Disabling Multicast Flooding During a TCN Event, page 18-12](#)

### Controlling the Multicast Flooding Time After a TCN Event

You can control the time that multicast traffic is flooded after a TCN event by using the **ip igmp snooping tcn flood query count** global configuration command. This command configures the number of general queries for which multicast data traffic is flooded after a TCN event. Some examples of TCN events are when the client changed its location and the receiver is on same port that was blocked but is now forwarding, and when a port went down without sending a leave message.

If you set the TCN flood query count to 1 by using the **ip igmp snooping tcn flood query count** command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Beginning in privileged EXEC mode, follow these steps to configure the TCN flood query count:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping tcn flood query count <i>count</i></b>	Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10. By default, the flooding query count is 2.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show ip igmp snooping</b>	Verify the TCN settings.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default flooding query count, use the **no ip igmp snooping tcn flood query count** global configuration command.

## Recovering from Flood Mode

When a topology change occurs, the spanning-tree root sends a special IGMP leave message (also known as global leave) with the group multicast address 0.0.0.0. However, when you enable the **ip igmp snooping tcn query solicit** global configuration command, the switch sends the global leave message whether or not it is the spanning-tree root. When the router receives this special leave, it immediately sends general queries, which expedite the process of recovering from the flood mode during the TCN event. Leaves are always sent if the switch is the spanning-tree root regardless of this configuration command. By default, query solicitation is disabled.

Beginning in privileged EXEC mode, follow these steps to enable the switch to send the global leave message whether or not it is the spanning-tree root:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping tcn query solicit</b>	Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event. By default, query solicitation is disabled.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show ip igmp snooping</b>	Verify the TCN settings.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default query solicitation, use the **no ip igmp snooping tcn query solicit** global configuration command.

## Disabling Multicast Flooding During a TCN Event

When the switch receives a TCN, multicast traffic is flooded to all the ports until 2 general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding might exceed the capacity of the link and cause packet loss. You can use the **ip igmp snooping tcn flood** interface configuration command to control this behavior.

Beginning in privileged EXEC mode, follow these steps to disable multicast flooding on an interface:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no ip igmp snooping tcn flood</b>	Disable the flooding of multicast traffic during a spanning-tree TCN event. By default, multicast flooding is enabled on an interface.
Step 4	<b>exit</b>	Return to privileged EXEC mode.
Step 5	<b>show ip igmp snooping</b>	Verify the TCN settings.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To re-enable multicast flooding on an interface, use the **ip igmp snooping tcn flood** interface configuration command.

## Configuring the IGMP Snooping Querier

Follow these guidelines when configuring the IGMP snooping querier:

- Configure the VLAN in global configuration mode.
- Configure an IP address on the VLAN interface. When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN switch virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the switch uses the first available IP address configured on the switch. The first IP address available appears in the output of the **show ip interface** privileged EXEC command. The IGMP snooping querier does not generate an IGMP general query if it cannot find an available IP address on the switch.
- The IGMP snooping querier supports IGMP Versions 1 and 2.
- When administratively enabled, the IGMP snooping querier moves to the nonquerier state if it detects the presence of a multicast router in the network.
- When it is administratively enabled, the IGMP snooping querier moves to the operationally disabled state under these conditions:
  - IGMP snooping is disabled in the VLAN.
  - PIM is enabled on the SVI of the corresponding VLAN.

Beginning in privileged EXEC mode, follow these steps to enable the IGMP snooping querier feature in a VLAN:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping querier</b>	Enable the IGMP snooping querier.
Step 3	<b>ip igmp snooping querier address</b> <i>ip_address</i>	(Optional) Specify an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.  <b>Note</b> The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the switch.
Step 4	<b>ip igmp snooping querier query-interval</b> <i>interval-count</i>	(Optional) Set the interval between IGMP queries. The range is 1 to 18000 seconds.
Step 5	<b>ip igmp snooping querier tcn query</b> [ <b>count</b> <i>count</i>   <b>interval</b> <i>interval</i> ]	(Optional) Set the time between Topology Change Notification (TCN) queries. The count range is 1 to 10. The interval range is 1 to 255 seconds.
Step 6	<b>ip igmp snooping querier timer expiry</b> <i>timeout</i>	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
Step 7	<b>ip igmp snooping querier version</b> <i>version</i>	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.
Step 8	<b>end</b>	Return to privileged EXEC mode.
Step 9	<b>show ip igmp snooping vlan</b> <i>vlan-id</i>	(Optional) Verify that the IGMP snooping querier is enabled on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094.
Step 10	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

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

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

## Disabling IGMP Report Suppression



### Note

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.

IGMP report suppression is enabled by default. When it is enabled, the switch forwards only one IGMP report per multicast router query. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers.

Beginning in privileged EXEC mode, follow these steps to disable IGMP report suppression:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>no ip igmp snooping report-suppression</b>	Disable IGMP report suppression.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show ip igmp snooping</b>	Verify that IGMP report suppression is disabled.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To re-enable IGMP report suppression, use the **ip igmp snooping report-suppression** global configuration command.

## Displaying IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

To display IGMP snooping information, use one or more of the privileged EXEC commands in Table 18-4.

**Table 18-4** Commands for Displaying IGMP Snooping Information

Command	Purpose
<code>show ip igmp snooping [vlan <i>vlan-id</i>]</code>	Display the snooping configuration information for all VLANs on the switch or for a specified VLAN.  (Optional) Enter <b>vlan</b> <i>vlan-id</i> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<code>show ip igmp snooping groups [count  dynamic [count]   user [count]]</code>	Display multicast table information for the switch or about a specific parameter: <ul style="list-style-type: none"> <li>• <b>count</b>—Display the total number of entries for the specified command options instead of the actual entries.</li> <li>• <b>dynamic</b>—Display entries learned through IGMP snooping.</li> <li>• <b>user</b>—Display only the user-configured multicast entries.</li> </ul>
<code>show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i>   count   dynamic [count]   user[count]]</code>	Display multicast table information for a multicast VLAN or about a specific parameter for the VLAN: <ul style="list-style-type: none"> <li>• <i>vlan-id</i>—The VLAN ID range is 1 to 1001 and 1006 to 4094.</li> <li>• <b>count</b>—Display the total number of entries for the specified command options instead of the actual entries.</li> <li>• <b>dynamic</b>—Display entries learned through IGMP snooping.</li> <li>• <i>ip_address</i>—Display characteristics of the multicast group with the specified group IP address.</li> <li>• <b>user</b>—Display only the user-configured multicast entries.</li> </ul>
<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	Display information on dynamically learned and manually configured multicast router interfaces.  <b>Note</b> When you enable IGMP snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces.  (Optional) Enter <b>vlan</b> <i>vlan-id</i> to display information for a single VLAN.
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>]</code>	Display information about the IP address and receiving port for the most-recently received IGMP query messages in the VLAN.  (Optional) Enter <b>vlan</b> <i>vlan-id</i> to display information for a single VLAN.
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>] detail</code>	Display information about the IP address and receiving port of the most-recently received IGMP query message in the VLAN and the configuration and operational state of the IGMP snooping querier in the VLAN.

For more information about the keywords and options in these commands, see the command reference for this release.

# Configuring IGMP Filtering and Throttling

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP is used to forward the multicast traffic.

IGMP filtering is applicable only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.

**Note**

---

IGMPv3 join and leave messages are not supported on switches running IGMP filtering.

---

These sections contain this configuration information:

- [Default IGMP Filtering and Throttling Configuration, page 18-17](#)
- [Configuring IGMP Profiles, page 18-17](#) (optional)
- [Applying IGMP Profiles, page 18-18](#) (optional)
- [Setting the Maximum Number of IGMP Groups, page 18-19](#) (optional)
- [Configuring the IGMP Throttling Action, page 18-19](#) (optional)

## Default IGMP Filtering and Throttling Configuration

Table 18-5 shows the default IGMP filtering configuration.

**Table 18-5** Default IGMP Filtering Configuration

Feature	Default Setting
IGMP filters	None applied
IGMP maximum number of IGMP groups	No maximum set
IGMP profiles	None defined
IGMP profile action	Deny the range addresses

When the maximum number of groups is in forwarding table, the default IGMP throttling action is to deny the IGMP report. For configuration guidelines, see the “[Configuring the IGMP Throttling Action](#)” section on page 18-19.

## Configuring IGMP Profiles

To configure an IGMP profile, use the **ip igmp profile** global configuration command with a profile number to create an IGMP profile and to enter IGMP profile configuration mode. From this mode, you can specify the parameters of the IGMP profile to be used for filtering IGMP join requests from a port. 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.
- **exit**: Exits from igmp-profile configuration mode.
- **no**: Negates a command or returns to its defaults.
- **permit**: Specifies that matching addresses are permitted.
- **range**: Specifies a range of IP addresses for the profile. You can enter a single IP address or a range with a start and an end address.

The default is for the switch to have no IGMP profiles configured. When a profile is configured, if neither the **permit** nor **deny** keyword is included, the default is to deny access to the range of IP addresses.

Beginning in privileged EXEC mode, follow these steps to create an IGMP profile:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp profile</b> <i>profile number</i>	Assign a number to the profile you are configuring, and enter IGMP profile configuration mode. The profile number range is 1 to 4294967295.
Step 3	<b>permit   deny</b>	(Optional) Set the action to permit or deny access to the IP multicast address. If no action is configured, the default for the profile is to deny access.

	Command	Purpose
Step 4	<b>range</b> <i>ip multicast address</i>	Enter the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address.  You can use the <b>range</b> command multiple times to enter multiple addresses or ranges of addresses.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp profile</b> <i>profile number</i>	Verify the profile configuration.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To delete a profile, use the **no ip igmp profile** *profile number* global configuration command.

To delete an IP multicast address or range of IP multicast addresses, use the **no range ip multicast address** IGMP profile configuration command.

This example shows how to create IGMP profile 4 allowing access to the single IP multicast address and how to verify the configuration. If the action was to deny (the default), it would not appear in the **show ip igmp profile** output display.

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

## Applying IGMP Profiles

To control access as defined in an IGMP profile, use the **ip igmp filter** interface configuration command to apply the profile to the appropriate interfaces. You can apply IGMP profiles only to Layer 2 access ports. You cannot apply profiles to ports that belong to an EtherChannel port group. You can apply a profile to multiple interfaces, but each interface can have only one profile applied to it.

Beginning in privileged EXEC mode, follow these steps to apply an IGMP profile to a switch port:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the physical interface, and enter interface configuration mode. The interface must be a Layer 2 port that does not belong to an EtherChannel port group.
Step 3	<b>ip igmp filter</b> <i>profile number</i>	Apply the specified IGMP profile to the interface. The range is 1 to 4294967295.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show running-config interface</b> <i>interface-id</i>	Verify the configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove a profile from an interface, use the **no ip igmp filter *profile number*** interface configuration command.

This example shows how to apply IGMP profile 4 to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

## Setting the Maximum Number of IGMP Groups

You can set the maximum number of IGMP groups that a Layer 2 interface can join by using the **ip igmp max-groups** interface configuration command. Use the **no** form of this command to set the maximum back to the default, which is no limit.

You can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

Beginning in privileged EXEC mode, follow these steps to set the maximum number of IGMP groups in the forwarding table:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the interface to be configured, and enter interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface.
Step 3	<b>ip igmp max-groups <i>number</i></b>	Set the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show running-config interface <i>interface-id</i></b>	Verify the configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the maximum group limitation and return to the default of no maximum, use the **no ip igmp max-groups** interface configuration command.

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

## Configuring the IGMP Throttling Action

After you set the maximum number of IGMP groups that a Layer 2 interface can join, you can configure an interface to replace the existing group with the new group for which the IGMP report was received by using the **ip igmp max-groups action replace** interface configuration command. Use the **no** form of this command to return to the default, which is to drop the IGMP join report.

Follow these guidelines when configuring the IGMP throttling action:

- You can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups action {deny | replace}** command has no effect.
- If you configure the throttling action and set the maximum group limitation after an interface has added multicast entries to the forwarding table, the forwarding-table entries are either aged out or removed, depending on the throttling action.
  - If you configure the throttling action as **deny**, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out and 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**, 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 entry with the received IGMP report.

To prevent the switch from removing the forwarding-table entries, you can configure the IGMP throttling action before an interface adds entries to the forwarding table.

Beginning in privileged EXEC mode, follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the physical interface to be configured, and enter interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or an EtherChannel interface. The interface cannot be a trunk port.
Step 3	<b>ip igmp max-groups action {deny   replace}</b>	When an interface receives an IGMP report and the maximum number of entries is in the forwarding table, specify the action that the interface takes: <ul style="list-style-type: none"> <li>• <b>deny</b>—Drop the report.</li> <li>• <b>replace</b>—Replace the existing group with the new group for which the IGMP report was received.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show running-config interface</b> <i>interface-id</i>	Verify the configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default action of dropping the report, use the **no ip igmp max-groups action** interface configuration command.

# Displaying IGMP Filtering and Throttling Configuration

You can display IGMP profile characteristics, and you can display the IGMP profile and maximum group configuration for all interfaces on the switch or for a specified interface. You can also display the IGMP throttling configuration for all interfaces on the switch or for a specified interface.

Use the privileged EXEC commands in [Table 18-6](#) to display IGMP filtering and throttling configuration:

**Table 18-6**      **Commands for Displaying IGMP Filtering and Throttling Configuration**

Command	Purpose
<b>show ip igmp profile</b> [ <i>profile number</i> ]	Displays the specified IGMP profile or all the IGMP profiles defined on the switch.
<b>show running-config</b> [ <b>interface</b> <i>interface-id</i> ]	Displays the configuration of the specified interface or the configuration of all interfaces on the switch, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface.

