CHAPTER 23

Configuring IGMP Snooping and Filtering

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 4500 series switch. It provides guidelines, procedures, and configuration examples.

This chapter consists of the following major sections:

Note To support Cisco Group Management Protocol (CGMP) client devices, configure the switch as a CGMP server. For more information, see the Cisco IOS 15.0M configuration guides at this location:

http://www.cisco.com/en/US/products/ps10591/products_installation_and_configuration_guides_list.html

Note For complete syntax and usage information for the switch commands used in this chapter, first look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

If the command is not found in the Catalyst 4500 Series Switch Command Reference, it will be found in the larger Cisco IOS library. Refer to the *Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

About IGMP Snooping

This section includes the following subsections:

- IGMP Snooping Querier, page 23-4
- Explicit Host Tracking, page 23-4

Note Quality of service does not apply to IGMP packets.

IGMP snooping allows a switch to snoop or capture information from IGMP packets transmitted between hosts and a router. Based on this information, a switch adds or deletes multicast addresses from its address table, which enables (or disables) multicast traffic from flowing to individual host ports. IGMP snooping supports all versions of IGMP: IGMPv1, IGMPv2, and IGMPv3.

In contrast to IGMPv1 and IGMPv2, IGMPv3 snooping provides immediate-leave processing by default. It provides explicit host tracking (EHT) and allows network administrators to deploy SSM functionality on Layer 2 devices that support IGMPv3. See the "Explicit Host Tracking" section on page 23-4. In subnets where IGMP is configured, IGMP snooping manages multicast traffic at Layer 2. You can configure interfaces to dynamically forward multicast traffic only to those interfaces that are interested in receiving it by using the **switchport** keyword.

IGMP snooping restricts traffic in MAC multicast groups 0100.5e00.0001 to 01-00-5e-ff-ff-ff. IGMP snooping does not restrict Layer 2 multicast packets generated by routing protocols.

Note For more information on IP multicast and IGMP, refer to RFC 1112, RFC 2236, RFC 3376 (for IGMPv3).

IGMP (configured on a router) periodically sends out IGMP general queries. A host responds to these queries with IGMP membership reports for groups that it is interested in. When IGMP snooping is enabled, the switch creates one entry per-VLAN in the Layer 2 forwarding table for each Layer 2 multicast group from which it receives an IGMP join request. All hosts interested in this multicast traffic send IGMP membership reports and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **ip igmp snooping static** command. If you specify group membership statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can contain both user-defined and IGMP snooping settings.

Groups with IP addresses in the range 224.0.0.0 to 224.0.0.255, which map to the multicast MAC address range 0100.5E00.0001 to 0100.5E00.00FF, are reserved for routing control packets. These groups are flooded to all forwarding ports of the VLAN with the exception of 224.0.0.22, which is used for IGMPv3 membership reports.

Note If a VLAN experiences a spanning-tree topology change, IP multicast traffic floods on all VLAN ports where PortFast is not enabled, as well as on ports with the **no igmp snooping tcn flood** command configured for a period of TCN query count.

For a Layer 2 IGMPv2 host interface to join an IP multicast group, a host sends an IGMP membership report for the IP multicast group. For a host to leave a multicast group, it can either ignore the periodic IGMP general queries or it can send an IGMP leave message. When the switch receives an IGMP leave message from a host, it sends out an IGMP group-specific query to determine whether any devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the table entry for that Layer 2 multicast group so that only those hosts interested in receiving multicast traffic for the group are listed.

In contrast, IGMPv3 hosts send IGMPv3 membership reports (with the **allow** group record mode) to join a specific multicast group. When IGMPv3 hosts send membership reports (with the **block** group record) to reject traffic from all sources in the previous source list, the last host on the port is removed by immediate-leave if EHT is enabled.

Immediate-Leave Processing

IGMP snooping immediate-leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out IGMP group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original IGMP leave message. Immediate-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are being used simultaneously.

When a switch with IGMP snooping enabled receives an IGMPv2 or IGMPv3 leave message, it sends an IGMP group-specific query from the interface where the leave message was received to determine when other hosts are attached to that interface that are interested in joining the MAC multicast group. If the switch does not receive an IGMP join message within the query response interval, the interface is removed from the port list of the (MAC-group, VLAN) entry in the Layer 2 forwarding table.

Note By default all IGMP joins are forwarded to all multicast router ports.

With immediate-leave processing enabled on the VLAN, an interface can be removed immediately from the port list of the Layer 2 entry when the IGMP leave message is received, unless a multicast router was learned on the port.

Note When using IGMPv2 snooping, use immediate-leave processing only on VLANs where just one host is connected to each interface. If immediate-leave processing is enabled on VLANs where multiple hosts are connected to an interface, some hosts might be dropped inadvertently. When using IGMPv3, immediate-leave processing is enabled by default, and due to explicit host tracking, the switch can detect when a port has single or multiple hosts maintained by the switch for IGMPv3 hosts. As a result, the switch can perform immediate-leave processing when it detects a single host behind a given port.

Note IGMPv3 is interoperable with older versions of IGMP.

To display the IGMP version on a particular VLAN, use the **show ip igmp snooping querier vlan** command.

To display whether the switch supports IGMPv3 snooping, use the **show ip igmp snooping vlan** command.

To enable immediate-leave for IGMPv2, use the **ip igmp snooping immediate-leave** command.

Note Immediate-leave processing is enabled by default for IGMPv3.

IGMP Configurable-Leave Timer

Immediate-leave processing cannot be used on VLANs where multiple hosts may be connected to a single interface. To reduce leave latency in such a scenario, IGMPv3 provides a configurable leave timer.

You can configure the length of 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 per-VLAN. The VLAN configuration of the leave time overrides the global configuration.

For configuration steps, see the "Configuring the IGMP Leave Timer" section on page 23-9.

IGMP Snooping Querier

IGMP Snooping Querier is a Layer 2 feature required to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not require routing.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier by sending general queries. If the IP-multicast traffic in a VLAN only needs to be Layer 2-switched, an IP-multicast router is not required. Without an IP-multicast router on the VLAN, you must configure another switch as the IGMP querier so that it can send queries.

When enabled, the IGMP snooping querier sends out periodic IGMPv2 queries that trigger IGMP report messages from the switch that requests IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

On switches that use IGMP to report interest in IP multicast traffic, configure at least one switch as the IGMP snooping querier in each supported VLAN.

You can configure a switch to generate IGMP queries on a VLAN regardless of whether IP multicast routing is enabled.

Explicit Host Tracking

Explicit host tracking (EHT) monitors group membership by tracking hosts that are sending IGMPv3 membership reports. This tracking enables a switch to detect host information associated with the groups of each port. EHT also enables the user to track the membership and various statistics.

EHT enables a switch to track membership on a per-port basis. Consequently, a switch is aware of the hosts residing on each port and can perform immediate-leave processing when there is only one host behind a port.

To determine whether EHT is enabled on a VLAN, use the **show ip igmp snoop vlan** command.

Configuring IGMP Snooping

Note When configuring IGMP, configure the VLAN in the VLAN database mode. See Chapter 13, "Configuring VLANs, VTP, and VMPS."

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

These sections describe how to configure IGMP snooping:

Default IGMP Snooping Configuration

Table 23-1 shows the IGMP snooping default configuration values.

Table 23-1 IGMP Snooping Default Configuration Values

Feature	Default Value
IGMP snooping	Enabled
Multicast routers	None configured
Explicit Host Tracking	Enabled for IGMPv3; Not available for IGMPv2
Immediate-leave processing	Enabled for IGMPv3; Disabled for IGMPv2
Report Suppression	Enabled
IGMP snooping learning method	PIM/DVMRP[1]

1. PIM/DVMRP = Protocol Independent Multicast/Distance Vector Multicast Routing Protocol

Enabling IGMP Snooping Globally

To enable IGMP snooping globally, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] ip igmp snooping`	Enables IGMP snooping. Use the **no** keyword to disable IGMP snooping.
Step 3	`Switch(config)# end`	Exits configuration mode.
Step 4	`Switch# show ip igmp snooping | include`	Verifies the configuration.

This example shows how to enable IGMP snooping globally and verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)# end
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2

Vlan 1:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled
Explicit host tracking         : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode     : IGMP_ONLY

Vlan 2:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled
Explicit host tracking         : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode     : IGMP_ONLY
```

Enabling IGMP Snooping on a VLAN

To enable IGMP snooping on a VLAN, perform this task:

	Command	Purpose
Step 1	`Switch(config)# [no] ip igmp snooping vlan vlan_ID`	Enables IGMP snooping. Use the **no** keyword to disable IGMP snooping.
Step 2	`Switch(config)# end`	Exits configuration mode.
Step 3	`Switch# show ip igmp snooping vlan vlan_ID`	Verifies the configuration.

This example shows how to enable IGMP snooping on VLAN 2 and verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 2
Switch(config)# end
Switch# show ip igmp snooping vlan 2
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2
```

```
Vlan 2:
--------
IGMP snooping                   : Enabled
IGMPv2 immediate leave          : Disabled
Explicit host tracking          : Enabled
Multicast router learning mode  : pim-dvmrp
CGMP interoperability mode      : IGMP_ONLY
```

Configuring Learning Methods

The following sections describe IGMP snooping learning methods:

- Configuring PIM/DVMRP Learning, page 23-7
- Configuring CGMP Learning, page 23-7

Configuring PIM/DVMRP Learning

To configure IGMP snooping to learn from PIM/DVMRP packets, perform this task:

Command	Purpose
Switch(config)# **ip igmp snooping vlan** *vlan_ID* **mrouter learn** [**cgmp** | **pim-dvmrp**]	Specifies the learning method for the VLAN.

This example shows how to configure IP IGMP snooping to learn from PIM/DVMRP packets:

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

Configuring CGMP Learning

To configure IGMP snooping to learn from CGMP self-join packets, perform this task:

Command	Purpose
Switch(config)# **ip igmp snooping vlan** *vlan_ID* **mrouter learn** [**cgmp** | **pim-dvmrp**]	Specifies the learning method for the VLAN.

This example shows how to configure IP IGMP snooping to learn from CGMP self-join packets:

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

Configuring a Static Connection to a Multicast Router

To configure a static connection to a multicast router, enter the **ip igmp snooping vlan mrouter interface** command on the switch.

To configure a static connection to a multicast router, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip igmp snooping vlan vlan_ID mrouter interface interface_num`	Specifies a static connection to a multicast router for the VLAN. **Note** The interface to the router must be in the VLAN where you are entering the command. The router and the line protocol must be up.
Step 3	`Switch(config)# end`	Exits configuration mode.
Step 4	`Switch# show ip igmp snooping mrouter vlan vlan_ID`	Verifies the configuration.

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface fastethernet 2/10
Switch# show ip igmp snooping mrouter vlan 200
vlan   ports
-----+---------------------------------------
 200   Fa2/10
Switch#
```

Enabling IGMP Immediate-Leave Processing

When you enable IGMP immediate-leave processing on a VLAN, a switch removes an interface from the multicast group when it detects an IGMPv2 leave message on that interface.

Note For IGMPv3, immediate-leave processing is enabled by default with EHT.

To enable immediate-leave processing on an IGMPv2 interface, perform this task:

Command	Purpose
`Switch(config)# ip igmp snooping vlan vlan_ID immediate-leave`	Enables immediate-leave processing in the VLAN. **Note** This command applies only to IGMPv2 hosts.

This example shows how to enable IGMP immediate-leave processing on interface VLAN 200 and to verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 immediate-leave
Configuring immediate leave on vlan 200
Switch(config)# end
Switch# show ip igmp interface vlan 200 | include immediate leave
Immediate leave                : Disabled
Switch(config)#
```

Configuring the IGMP Leave Timer

Follows these guidelines when configuring the IGMP leave timer:

- You can configure the leave time globally or per-VLAN.
- 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.

To enable the IGMP configurable-leave timer, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip igmp snooping last-member-query-interval` *time*	Configures the IGMP leave timer globally. The range is 100 to 5000 milliseconds. The default is 1000 seconds. To globally reset the IGMP leave timer to the default setting, use the global configuration command **no ip igmp snooping last-member-query-interva**l.
Step 3	`Switch(config)# ip igmp snooping vlan` *vlan_ID* `last-member-query-interval` *time*	(Optional) Configures the IGMP leave time on the VLAN interface. The range is 100 to 5000 milliseconds. To remove the configured IGMP leave-time setting from the specified VLAN, use the global configuration command **no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** **Note** Configuring the leave time on a VLAN overrides the globally configured timer.
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show ip igmp snooping`	(Optional) Displays the configured IGMP leave time.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to enable the IGMP configurable-leave timer and to verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping last-member-query-interval 200
Switch(config)# ip igmp snooping vlan 10 last-member-query-interval 500
Switch(config)# end
Switch# show ip igmp snooping show ip igmp snooping
Global IGMP Snooping configuration:
--------------------------------

IGMP snooping              : Enabled
IGMPv3 snooping            : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last Member Query Interval : 200

Vlan 1:
```

```
--------
IGMP snooping                          : Enabled
IGMPv2 immediate leave                 : Disabled
Explicit host tracking                 : Enabled
Multicast router learning mode         : pim-dvmrp
Last Member Query Interval             : 200
CGMP interoperability mode             : IGMP_ONLY

Vlan 10:
--------
IGMP snooping                          : Enabled
IGMPv2 immediate leave                 : Disabled
Explicit host tracking                 : Enabled
Multicast router learning mode         : pim-dvmrp
Last Member Query Interval             : 500
CGMP interoperability mode             : IGMP_ONLY

Switch#
```

Configuring IGMP Snooping Querier

The IGMP Snooping Querier feature can be enabled either globally or per-VLAN.

Note The IGMP snooping querier is disabled by default.

To configure IGMP Snooping Querier, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] ip igmp snooping [vlan vlan_id] querier`	Enables IGMP Snooping Querier.
Step 3	`Switch(config)# [no] ip igmp snooping [vlan vlan_id] querier address abcd`	Configures the IGMP Snooping Querier source IP address.
Step 4	`Switch(config)# [no] ip igmp snooping [vlan vlan_id] querier version [1 | 2]`	Configures IGMP Snooping Querier IGMP version.
Step 5	`Switch(config)# ip igmp snooping [vlan vlan_id] querier query-interval interval`	Configures IGMP Snooping Querier query interval.
Step 6	`Switch(config)# ip igmp snooping [vlan vlan_id] querier max-response-time value`	Configures IGMP Snooping Querier query maximum response time.
Step 7	`Switch(config)# ip igmp snooping [vlan vlan_id] querier timer expiry value`	Configures IGMP Snooping Querier expiry time out.
Step 8	`Switch(config)# ip igmp snooping [vlan vlan_id] querier tcn query count value`	Configures IGMP Snooping Querier tcn query count.
Step 9	`Switch(config)# ip igmp snooping [vlan vlan_id] querier tcn query interval value`	Configures IGMP Snooping Querier tcn query interval.
Step 10	`Switch(config)# end`	Returns to privileged EXEC mode.

For an example of how to display Snooping Querier information, refer to the "Displaying IGMP Snooping Querier Information" section on page 23-18.

Configuring Explicit Host Tracking

For IGMPv3, EHT is enabled by default and can be disabled on a per-VLAN basis.

To disable EHT processing on a VLAN, perform this task:

Command	Purpose
`Switch(config)# [no] ip igmp snooping vlan vlan_ID explicit-tracking`	Enables EHT on a VLAN. The **no** keyword disables EHT.

This example shows how to disable IGMP EHT on VLAN 200 and to verify the configuration:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
Switch# show ip igmp snooping vlan 200 | include Explicit host tracking
Explicit host tracking         : Disabled
```

Configuring a Host Statically

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

To configure a host statically on an interface, perform this task:

Command	Purpose
`Switch(config-if)# ip igmp snooping vlan vlan_ID static mac_address interface interface_num`	Configures a host statically in the VLAN. **Note** This command cannot be configured to receive traffic for specific source IP addresses.

This example shows how to configure a host statically in VLAN 200 on interface Fast Ethernet 2/11:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 static 0100.5e02.0203 interface fastethernet
2/11
Configuring port FastEthernet2/11 on group 0100.5e02.0203 vlan 200
Switch(config)# end
```

Suppressing Multicast Flooding

An IGMP snooping-enabled switch floods multicast traffic to all ports in a VLAN when a spanning-tree topology change notification (TCN) is received. Multicast flooding suppression enables a switch to stop sending such traffic. To support flooding suppression, the following interface and global commands were introduced:

- [**no** | **default**] **ip igmp snooping tcn flood** (interface command)
- [**no** | **default**] **ip igmp snooping tcn flood query count** [*1 - 10*] (global command)
- [**no** | **default**] **ip igmp snooping tcn query solicit** (global command)

This flooding behavior is undesirable if the switch that does the flooding has many ports that are subscribed to different groups. The traffic could exceed the capacity of the link between the switch and the end host, resulting in packet loss.

With the **no ip igmp snooping tcn flood** command, you can disable multicast flooding on a switch interface following a topology change. Only the multicast groups that have been joined by a port are sent to that port, even during a topology change.

With the **ip igmp snooping tcn flood query count** command, you can enable multicast flooding on a switch interface for a short period of time following a topology change by configuring an IGMP query threshold.

Typically, if a topology change occurs, the spanning tree root switch issues a global IGMP leave message (referred to as a "query solicitation") with the group multicast address 0.0.0.0. When a switch receives this solicitation, it floods this solicitation on all ports in the VLAN where the spanning tree change occurred. When the upstream router receives this solicitation, it immediately issues an IGMP general query.

With the **ip igmp snooping tcn query solicit** command, you can now direct a non-spanning tree root switch to enter the same query solicitation.

The following sections provide additional details on the new commands and illustrate how you can use them.

IGMP Snooping Interface Configuration

A topology change in a VLAN may invalidate previously learned IGMP snooping information. A host that was on one port before the topology change may move to another port after the topology change. When the topology changes, the Catalyst 4500 series switch takes special actions to ensure that multicast traffic is delivered to all multicast receivers in that VLAN.

When the spanning tree protocol is running in a VLAN, a spanning tree topology change notification (TCN) is issued by the root switch in the VLAN. A Catalyst 4500 series switch that receives a TCN in a VLAN for which IGMP snooping has been enabled immediately enters into multicast flooding mode for a period of time until the topology restabilizes and the new locations of all multicast receivers are learned.

While in multicast flooding mode, IP multicast traffic is delivered to all ports in the VLAN, and not restricted to those ports on which multicast group members have been detected.

You can manually prevent IP multicast traffic from being flooded to a switch port by using the **no ip igmp snooping tcn flood** command on that port.

For trunk ports, the configuration applies to all VLANs.

By default, multicast flooding is enabled. Use the **no** keyword to disable flooding, and use **default** to restore the default behavior (flooding is enabled).

To disable multicast flooding on an interface, perform this task:

	Command	Purpose
Step 1	`Switch(config)# interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port`	Selects the interface to configure.
Step 2	`Switch(config-if)# no ip igmp snooping tcn flood`	Disables multicast flooding on the interface when TCNs are received by the switch. To enable multicast flooding on the interface, enter this command: **default ip igmp snooping tcn flood**
Step 3	`Switch(config)# end`	Exits configuration mode.
Step 4	`Switch# show running interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port`	Verifies the configuration.

This example shows how to disable multicast flooding on interface Fast Ethernet 2/11:

```
Switch(config)# interface fastethernet 2/11
Switch(config-if)# no ip igmp snooping tcn flood
Switch(config-if)# end
Switch#
```

IGMP Snooping Switch Configuration

By default, flooding mode persists until the switch receives two IGMP general queries. You can change this period of time by using the **ip igmp snooping tcn flood query count** *n* command, where *n* is a number between 1 and 10.

This command operates at the global configuration level.

The default number of queries is 2. The **no** and **default** keywords restore the default.

To establish an IGMP query threshold, perform this task:

	Command	Purpose
Step 1	`Switch(config)# ip igmp snooping tcn flood query count <n>`	Modifies the number of IGMP queries the switch waits for before it stops flooding multicast traffic. To return the switch to the default number of IGMP queries, enter this command**:** **default ip igmp snooping tcn flood query count** .
Step 2	`Switch(config)# end`	Exits configuration mode.

This example shows how to modify the switch to stop flooding multicast traffic after four queries:

```
Switch(config)# ip igmp snooping tcn flood query count 4
Switch(config)# end
Switch#
```

When a spanning tree root switch receives a topology change in an IGMP snooping-enabled VLAN, the switch issues a query solicitation that causes an Cisco IOS router to send out one or more general queries. The new command **ip igmp snooping tcn query solicit** causes the switch to send the query solicitation whenever it notices a topology change, even if that switch is not the spanning tree root.

This command operates at the global configuration level.

By default, query solicitation is disabled unless the switch is the spanning tree root. The **default** keyword restores the default behavior.

To direct a switch to send a query solicitation, perform this task:

	Command	Purpose
Step 1	`Switch(config)# ip igmp snooping tcn query solicit`	Configures the switch to send a query solicitation when a TCN is detected. To stop the switch from sending a query solicitation (if it is not a spanning tree root switch), enter the **no ip igmp snooping tcn query solicit** command.
Step 2	`Switch(config)# end`	Exits configuration mode.

This example shows how to configure the switch to send a query solicitation upon detecting a TCN:

```
Switch(config)# ip igmp snooping tcn query solicit
Switch(config)# end
Switch#
```

Displaying IGMP Snooping Information

The following sections show how to display IGMP snooping information:

- Displaying Querier Information, page 23-14
- Displaying IGMP Host Membership Information, page 23-15
- Displaying Group Information, page 23-16
- Displaying Multicast Router Interfaces, page 23-17
- Displaying MAC Address Multicast Entries, page 23-17
- Displaying IGMP Snooping Information on a VLAN Interface, page 23-18
- Configuring IGMP Filtering, page 23-19

Displaying Querier Information

To display querier information, perform this task:

Command	Purpose
`Switch# show ip igmp snooping querier [vlan` *vlan_ID*`]`	Displays multicast router interfaces.

This example shows how to display the IGMP snooping querier information for all VLANs on the switch:

```
Switch# show ip igmp snooping querier
Vlan      IP Address      IGMP Version        Port
-----------------------------------------------------
2         10.10.10.1      v2                  Router
3         172.20.50.22    v3                  Fa3/15
```

This example shows how to display the IGMP snooping querier information for VLAN 3:

```
Switch# show ip igmp snooping querier vlan 3
Vlan      IP Address     IGMP Version        Port
-------------------------------------------------
3         172.20.50.22   v3                  Fa3/15
```

Displaying IGMP Host Membership Information

Note By default, EHT maintains a maximum of 1000 entries in the EHT database. Once this limit is reached, no additional entries are created. To create additional entries, clear the database with the **clear ip igmp snooping membership vlan** command.

To display host membership information, perform this task:

Command	Purpose
Switch# **show ip igmp snooping membership** [**interface** *interface_num*][**vlan** *vlan_ID*] [**reporter** *a.b.c.d*] [**source** *a.b.c.d* **group** *a.b.c.d*]	Displays EHT information. **Note** This command is valid only if EHT is enabled on the switch.

This example shows how to display host membership information for VLAN 20 and to delete the EHT database:

```
Switch# show ip igmp snooping membership vlan 20
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.3/224.10.10.10 Gi4/2 20.20.2020 00:23:37 00:06:50 00:20:30
40.40.40.4/224.10.10.10Gi4/1 20.20.20.20 00:39:42 00:09:17 -

40.40.40.5/224.10.10.10Fa2/1 20.20.20.20 00:39:42 00:09:17 -
40.40.40.6/224.10.10.10 Fa2/1 20.20.20.20 00:09:47 00:09:17 -

Switch# clear ip igmp snooping membership vlan 20
```

This example shows how to display host membership for interface gi4/1:

```
Switch# show ip igmp snooping membership interface gi4/1
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.4/224.10.10.10Gi4/1 20.20.20.20 00:39:42 00:09:17 -
```

This example shows how to display host membership for VLAN 20 and group 224.10.10.10:

```
Switch# show ip igmp snooping membership vlan 20 source 40.40.40.2 group 224.10.10.10
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
```

Displaying Group Information

To display detailed IGMPv3 information associated with a group, perform one of the following tasks:

Command	Purpose
`Switch# show ip igmp snooping groups [vlan vlan_ID]`	Displays groups, the type of reports that were received for the group (Host Type), and the list of ports on which reports were received. The report list includes neither the multicast router ports nor the complete forwarding port set for the group. It lists the ports on which the reports have been received. To display the complete forwarding port set for the group, display the CLI output for the MAC address that maps to this group by using the **show mac-address-table multicast** command.
`Switch# show ip igmp snooping groups [vlan vlan_ID a.b.c.d] [summary|sources|hosts]`	Displays information specific to a group address, providing details about the current state of the group with respect to sources and hosts. **Note** This command applies only to full IGMPv3 snooping support and can be used for IGMPv1, IGMPv2, or IGMPv3 groups.
`Switch# show ip igmp snooping groups [vlan vlan_ID] [count]`	Displays the total number of group addresses learned by the system on a global or per-VLAN basis.

This example shows how to display the host types and ports of a group in VLAN 1:

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7
Vlan      Group           Version     Ports
------------------------------------------------------
10        226.6.6.7       v3          Fa7/13, Fa7/14
Switch>
```

This example shows how to display the current state of a group with respect to a source IP address:

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7 sources
Source information for group 226.6.6.7:
Timers: Expired sources are deleted on next IGMP General Query

SourceIP       Expires   Uptime    Inc Hosts Exc Hosts
------------------------------------------------------
2.0.0.1        00:03:04  00:03:48  2         0
2.0.0.2        00:03:04  00:02:07  2         0
Switch>
```

This example shows how to display the current state of a group with respect to a host MAC address:

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7 hosts
IGMPv3 host information for group 226.6.6.7
Timers: Expired hosts are deleted on next IGMP General Query

Host (MAC/IP)  Filter mode    Expires   Uptime    # Sources
------------------------------------------------------------
```

```
175.1.0.29      INCLUDE         stopped   00:00:51       2
175.2.0.30      INCLUDE         stopped   00:04:14       2
```

This example shows how to display summary information for an IGMPv3 group:

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7 summary
Group Address (Vlan 10)         : 226.6.6.7
Host type                       : v3
Member Ports                    : Fa7/13, Fa7/14
Filter mode                     : INCLUDE
Expires                         : stopped
Sources                         : 2
Reporters (Include/Exclude)     : 2/0
```

This example shows how to display the total number of group addresses learned by the system globally:

```
Switch# show ip igmp snooping groups count
    Total number of groups:   54
```

This example shows how to display the total number of group addresses learned on VLAN 5:

```
Switch# show ip igmp snooping groups vlan 5 count
    Total number of groups:   30
```

Displaying Multicast Router Interfaces

When you enable IGMP snooping, the switch automatically learns to which interface the multicast routers are connected.

To display multicast router interfaces, perform this task:

Command	Purpose
Switch# **show ip igmp snooping mrouter vlan** *vlan_ID*	Displays multicast router interfaces.

This example shows how to display the multicast router interfaces in VLAN 1:

```
Switch# show ip igmp snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
Switch#
```

Displaying MAC Address Multicast Entries

To display MAC address multicast entries for a VLAN, perform this task:

Command	Purpose
Switch# **show mac-address-table multicast vlan** *vlan_ID* [**count**]	Displays MAC address multicast entries for a VLAN.

This example shows how to display MAC address multicast entries for VLAN 1:

```
Switch# show mac-address-table multicast vlan 1
```

```
Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------
   1    0100.5e01.0101     igmp Switch,Gi6/1
   1    0100.5e01.0102     igmp Switch,Gi6/1
   1    0100.5e01.0103     igmp Switch,Gi6/1
   1    0100.5e01.0104     igmp Switch,Gi6/1
   1    0100.5e01.0105     igmp Switch,Gi6/1
   1    0100.5e01.0106     igmp Switch,Gi6/1
Switch#
```

This example shows how to display a total count of MAC address entries for VLAN 1:

```
Switch# show mac-address-table multicast vlan 1 count
Multicast MAC Entries for vlan 1:    4
Switch#
```

Displaying IGMP Snooping Information on a VLAN Interface

To display IGMP snooping information on a VLAN, perform this task:

Command	Purpose
`Switch# show ip igmp snooping vlan vlan_ID`	Displays IGMP snooping information on a VLAN interface.

This example shows how to display IGMP snooping information on VLAN 5:

```
Switch# show ip igmp snooping vlan 5
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             :Enabled
IGMPv3 snooping support   :Full
Report suppression        :Enabled
TCN solicit query         :Disabled
TCN flood query count     :2

Vlan 5:
--------
IGMP snooping                  :Enabled
Immediate leave                :Disabled
Explicit Host Tracking         :Disabled
Multicast router learning mode :pim-dvmrp
CGMP interoperability mode     :IGMP_ONLY
```

Displaying IGMP Snooping Querier Information

To display IGMP Snooping Querier information, perform this task:

Command	Purpose
`Switch# show ip igmp snooping querier [vlan vlan_ID] [detail]`	Displays the IGMP Snooping Querier state.

This example shows how to display Snooping Querier information:

```
switch# show ip igmp snooping querier vlan 2 detail
IP address                  : 1.2.3.4
IGMP version               : v2
Port                         : Router/Switch
Max response time        : 12s


Global IGMP switch querier status
-------------------------------------------------
admin state                  : Enabled
admin version                : 2
source IP address            : 1.2.3.4
query-interval (sec)         : 130
max-response-time (sec)   : 10
querier-timeout (sec)         : 100
tcn query count              : 2
tcn query interval (sec)     : 10

Vlan 2:   IGMP switch querier status
-------------------------------------------------
admin state                          : Enabled
admin version                     : 2
source IP address               : 1.2.3.4
query-interval (sec)            : 55
max-response-time (sec)    : 12
querier-timeout (sec)          : 70
tcn query count                   : 10
tcn query interval (sec)       : 8
operational state                  : Querier
operational version              : 2
tcn query pending count      : 0
```

Configuring IGMP Filtering

This section includes the following subsections:

Note The IGMP filtering feature works for IGMPv1 and IGMPv2 only.

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

With the IGMP filtering feature, an administrator can use this type of control. With this 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.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

You can also set the maximum number of IGMP groups that a Layer 2 interface can join with the **ip igmp max-groups** *n* command.

Default IGMP Filtering Configuration

Table 23-2 shows the default IGMP filtering configuration.

Table 23-2 Default IGMP Filtering Settings

Feature	Default Setting
IGMP filters	No filtering
IGMP maximum number of IGMP groups	No limit
IGMP profiles	None defined

Configuring IGMP Profiles

To configure an IGMP profile and to enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command. From the IGMP profile configuration 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 using these commands:

- **deny—**Specifies that matching addresses are denied (the default condition).
- **exit**—Exits from igmp-profile configuration mode.
- **no—**Negates a command or sets 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 starting and ending addresses.

By default, no IGMP profiles are configured. When a profile is configured with neither the **permit** nor the **deny** keyword, the default is to deny access to the range of IP addresses.

To create an IGMP profile for a port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip igmp profile` *profile number*	Enters IGMP profile configuration mode and assigns a number to the profile you are configuring. The range is from 1 to 4,294,967,295.
Step 3	`Switch(config-igmp-profile)# permit | deny`	(Optional) Sets 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	`Switch(config-igmp-profile)# range` *ip multicast address*	Enters 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. Use the **range** command multiple times to enter multiple addresses or ranges of addresses.
Step 5	`Switch(config-igmp-profile)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# show ip igmp profile` *profile-number*	Verifies the profile configuration.
Step 7	`Switch# copy running-config startup-config`	(Optional) Saves 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 were to deny (the default), it does not appear in the output of the **show ip igmp profile** command.

```
Switch# configure terminal
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 a profile to multiple interfaces, but each interface can only have one profile applied to it.

Note You can apply IGMP profiles to Layer 2 ports only. You cannot apply IGMP profiles to routed ports (or SVIs) or to ports that belong to an EtherChannel port group.

To apply an IGMP profile to a switch port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode, and enters the physical interface to configure, for example, **fastethernet2/3**. The interface must be a Layer 2 port that does not belong to an EtherChannel port group.
Step 3	`Switch(config-if)# ip igmp filter` *profile number*	Applies the specified IGMP profile to the interface. The profile number can be from 1 to 4,294,967,295.

	Command	Purpose
Step 4	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show running configuration interface` *interface-id*	Verifies the configuration.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

This example shows how to apply IGMP profile 4 to an interface and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
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.

Note This restriction can be applied to Layer 2 ports only. You cannot set a maximum number of IGMP groups on routed ports (or SVIs) or on ports that belong to an EtherChannel port group.

To apply an IGMP profile on a switch port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode, and enter the physical interface to configure, for example, **gigabitethernet1/1**. The interface must be a Layer 2 port that does not belong to an EtherChannel group.
Step 3	`Switch(config-if)# ip igmp max-groups` *number*	Sets the maximum number of IGMP groups that the interface can join. The range is from 0 to 4,294,967,294. By default, no maximum is set. To remove the maximum group limitation and return to the default of no maximum, use the **no ip igmp max-groups** command.
Step 4	`Switch(config-if)# end`	Returns to privileged EXEC mode.

	Command	Purpose
Step 5	`Switch# show running-configuration interface interface-id`	Verifies the configuration.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

```
Switch# configure terminal
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```

Displaying IGMP Filtering Configuration

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

To display IGMP profiles, perform this task:

Command	Purpose
`Switch# show ip igmp profile [profile number]`	Displays the specified IGMP profile or all IGMP profiles defined on the switch.

To display interface configuration, perform this task:

Command	Purpose
`Switch# show running-configuration [interface interface-id]`	Displays the configuration of the specified interface or 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.

This is an example of the **show ip igmp profile** privileged EXEC command when no profile number is entered. All profiles defined on the switch are displayed.

```
Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
```

```
    range 229.9.9.0 229.255.255.255
```

This is an example of the **show running-config** privileged EXEC command when an interface is specified with IGMP maximum groups configured and IGMP profile 4 has been applied to the interface:

```
Switch# show running-config interface fastethernet2/12
Building configuration...
Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```