Configuring IGMP Snooping for IPv4 Multicast Traffic

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping in Cisco IOS Release 12.2SX.

Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

- To constrain IPv6 Multicast traffic, see Chapter 36, "Configuring MLD Snooping for IPv6 Multicast Traffic."

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

This chapter consists of these sections:

Understanding IGMP Snooping

These sections describe IGMP snooping:

IGMP Snooping Overview

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it. With Release 12.2(33)SXJ2 and later releases, IGMP snooping also constrains multicast traffic to VPLS interfaces.

IGMP, which runs at Layer 3 on a multicast router, generates Layer 3 IGMP queries in subnets where the multicast traffic needs to be routed. For information about IGMP, see Chapter 37, "Configuring IPv4 Multicast Layer 3 Switching."

You can configure the IGMP snooping querier on the switch to support IGMP snooping in subnets that do not have any multicast router interfaces. For more information about the IGMP snooping querier, see the "Configuring the IGMP Snooping Querier" section on page 38-10.

IGMP (on a multicast router) or, locally, the IGMP snooping querier, sends out periodic general IGMP queries that the switch forwards through all ports in the VLAN and to which hosts respond. IGMP snooping monitors the Layer 3 IGMP traffic.

Note If a multicast group has only sources and no receivers in a VLAN, IGMP snooping constrains the multicast traffic to only the multicast router ports.

Joining a Multicast Group

Hosts join multicast groups either by sending an unsolicited IGMP join message or by sending an IGMP join message in response to a general query from a multicast router (the switch forwards general queries from multicast routers to all ports in a VLAN).

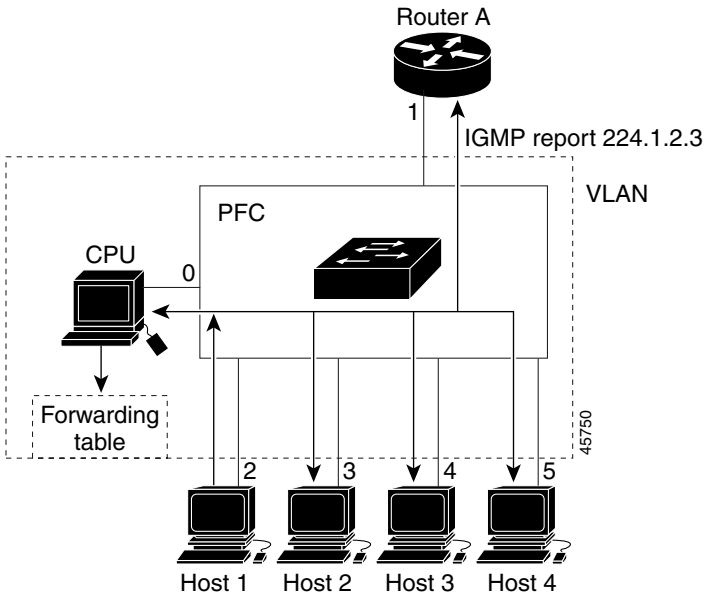
In response to an IGMP join request, the switch creates an entry in its Layer 2 forwarding table for the VLAN on which the join request was received. When other hosts that are interested in this multicast traffic send IGMP join requests, the switch adds them to the existing Layer 2 forwarding table entry. The switch creates only one entry per VLAN in the Layer 2 forwarding table for each multicast group for which it receives an IGMP join request.

IGMP snooping suppresses all but one of the host join messages per multicast group and forwards this one join message to the multicast router.

The switch forwards multicast traffic for the multicast group specified in the join message to the interfaces where join messages were received (see Figure 38-1).

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **mac-address-table static** command. When you specify group membership for a multicast group address statically, the static setting supersedes any IGMP snooping learning. Multicast group membership lists can consist of both static and IGMP snooping-learned settings.

Figure 38-1 Initial IGMP Join Message



Multicast router A sends a general query to the switch, which forwards the query to ports 2 through 5 (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 with the equivalent MAC destination address of 0x0100.5E01.0203. When the CPU receives the IGMP report multicast by Host 1, the CPU uses the information in the IGMP report to set up a forwarding-table entry, as shown in Table 38-1, that includes the port numbers of Host 1, the multicast router, and the switch internal CPU.

Table 38-1 IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2

The switch hardware can distinguish IGMP information packets from other packets for the multicast group. The first entry in the table tells the switching engine to send only IGMP packets to the CPU. This prevents the CPU from becoming overloaded with multicast frames. The second entry tells the switching engine to send frames addressed to the 0x0100.5E01.0203 multicast MAC address that are not IGMP packets (!IGMP) to the multicast router and to the host that has joined the group.

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group (Figure 38-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 38-2. Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports. Any known multicast traffic is forwarded to the group and not to the CPU.

Figure 38-2 Second Host Joining a Multicast Group

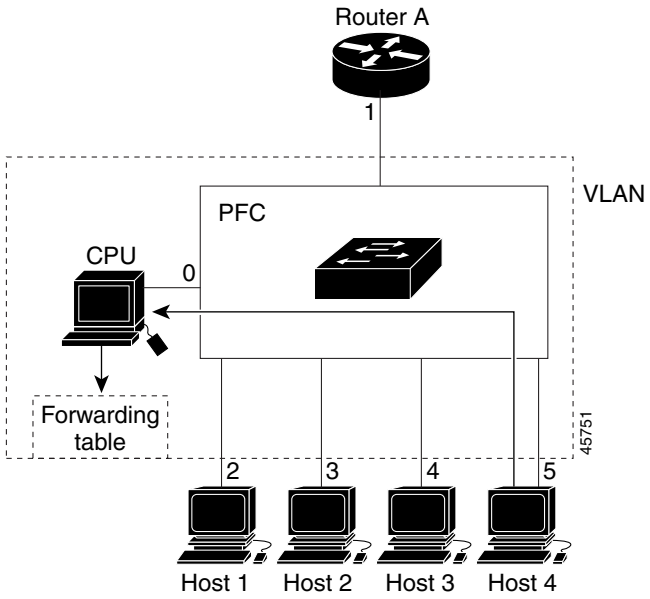


Table 38-2 Updated IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2, 5

Leaving a Multicast Group

These sections describe leaving a multicast group:

- Normal Leave Processing, page 38-4
- Fast-Leave Processing, page 38-5

Normal Leave Processing

Interested hosts must continue to respond to the periodic general IGMP queries. As long as at least one host in the VLAN responds to the periodic general IGMP queries, the multicast router continues forwarding the multicast traffic to the VLAN. When hosts want to leave a multicast group, they can either ignore the periodic general IGMP queries (called a “silent leave”), or they can send a group-specific IGMPv2 leave message.

When IGMP snooping receives a group-specific IGMPv2 leave message from a host, it sends out a MAC-based general query to determine if any other devices connected to that interface are interested in traffic for the specific multicast group. If IGMP snooping does not receive an IGMP Join message in response to the general query, it assumes that no other devices connected to the interface are interested in receiving traffic for this multicast group, and it removes the interface from its Layer 2 forwarding table entry for that multicast group. If the leave message was from the only remaining interface with hosts interested in the group and IGMP snooping does not receive an IGMP Join in response to the general

query, it removes the group entry and relays the IGMP leave to the multicast router. If the multicast router receives no reports from a VLAN, the multicast router removes the group for the VLAN from its IGMP cache.

The interval for which the switch waits before updating the table entry is called the "last member query interval," (See the "Configuring the IGMP Snooping Querier" section on page 38-10.)

Fast-Leave Processing

IGMP snooping fast-leave processing allows IGMP snooping to remove a Layer 2 LAN interface from the forwarding-table entry without first sending out IGMP group-specific queries to the interface. Upon receiving a group-specific IGMPv2 leave message, IGMP snooping immediately removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing improves bandwidth management for all hosts on a switched network.

Note Use fast-leave processing only on VLANs where only one host is connected to each Layer 2 LAN port. If fast-leave is enabled in VLANs where more than one host is connected to a Layer 2 LAN port, some hosts might be dropped inadvertently. Fast-leave processing is supported only with IGMP version 2 hosts.

Understanding the IGMP Snooping Querier

Use the IGMP snooping querier to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. If the IP-multicast traffic in a VLAN only needs to be Layer 2 switched, an IP-multicast router is not required, but 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 IGMPv3 queries that trigger IGMP report messages from the switch that wants to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

Configure one switch as the IGMP snooping querier in each VLAN that is supported on switches that use IGMP to report interest in IP multicast traffic.

Note Enable the IGMP snooping querier on only one switch in the VLAN.

You can configure a switch to generate IGMP queries on a VLAN regardless of whether or not IP multicast routing is enabled (see the "Configuring the IGMP Snooping Querier" section on page 38-10).

Understanding IGMP Version 3 Support

These sections describe IGMP version 3 support:

IGMP Version 3 Support Overview

IGMP snooping supports IGMP version 3 (IGMPv3). IGMPv3 uses source-based filtering, which enables hosts and routers to specify which source addresses should be allowed or blocked for a specific multicast group. When you enable IGMPv3 snooping, the switch maintains IGMPv3 states based on messages it receives for a particular group in a particular VLAN and either allows or blocks traffic based on the following information in these messages:

- Source lists
- Allow (include) or block (exclude) filtering options

Because the Layer 2 table is (MAC-group, VLAN) based, with IGMPv3 hosts it is preferable to have only a single multicast source per MAC-group.

Note Source-based filtering for IGMPv3 reports is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection. The source-only entries are deleted every 5 minutes and relearned to ensure that they are still valid.

IGMPv3 Fast-Leave Processing

IGMPv3 fast-leave processing is active if explicit-host tracking is enabled. The **ip igmp snooping fast-leave** command that enables IGMP version 2 fast-leave processing does not affect IGMPv3 fast-leave processing.

Fast-leave processing with IGMPv3 is implemented by maintaining source-group based membership information in software while also allocating LTL indexes on a MAC GDA basis.

When fast-leave processing is active, hosts send BLOCK_OLD_SOURCES{src-list} messages for a specific group when they no longer want to receive traffic from that source. When the switch receives such a message from a host, it parses the list of sources for that host for the given group. If this source list is exactly the same as the source list received in the leave message, the switch removes the host from the LTL index and stops forwarding this multicast group traffic to this host.

If the source lists do not match, the switch does not remove the host from the LTL index until the host is no longer interested in receiving traffic from any source.

Proxy Reporting

IGMP supports proxy reporting for IGMPv1 and IGMPv2 messages to handle group-specific queries. These queries are not sent downstream, but the switch does respond to them directly. When the switch receives a group-specific query, the switch terminates the query and sends an IGMP proxy report if there is a receiver for the group. There is no proxy reporting for IGMPv3 messages. For IGMPv3, a group-specific query or a group source-specific query is flooded to all VLAN member ports. The database for the IGMPv3 membership report is built based on the reports received.

Host reports responding to a specific query can be suppressed by the report suppression feature. Report suppression is supported for IGMPv1, IGMPv2, and IGMPv3 messages. With report suppression enabled (by default), when the switch receives a general query, the switch starts a suppression cycle for reports from all hosts to each group or channel (S,G). Only the first report to the discovered multicast

routers is forwarded; the rest of the reports are suppressed. For IGMPv1 and IGMPv2, the time of suppression is the report response time indicated in the general query message. For IGMPv3, suppression occurs for the entire general query interval.

Note

- Source-based filtering for IGMP version 3 reports is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection. The source-only entries are deleted every 5 minutes and relearned to ensure that they are still valid.
- Turning off explicit host tracking disables fast-leave processing and proxy reporting.

Explicit Host Tracking

IGMPv3 supports explicit tracking of membership information on any port. The explicit-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When explicit tracking is enabled on a VLAN, the IGMP snooping software processes the IGMPv3 report it receives from a host and builds an explicit-tracking database that contains the following information:

- The port connected to the host
- The channels reported by the host
- The filter mode for each group reported by the host
- The list of sources for each group reported by the hosts
- The router filter mode of each group
- For each group, the list of hosts requesting the source

Note

- Turning off explicit host tracking disables fast-leave processing and proxy reporting.
- When explicit tracking is enabled and the switch is working in proxy-reporting mode, the router may not be able to track all the hosts behind a VLAN interface.

Default IGMP Snooping Configuration

Table 38-3 shows the default IGMP snooping configuration.

Table 38-3 IGMP Snooping Default Configuration

Feature	Default Values
IGMP snooping querier	Disabled
IGMP snooping	Enabled
Multicast routers	None configured
IGMPv3 proxy reporting	Enabled
IGMP snooping router learning method	Learned automatically through PIM or IGMP packets
Fast-Leave Processing	Disabled

Table 38-3 IGMP Snooping Default Configuration (continued)

Feature	Default Values
CGMP Automatic Detection	Enabled
IGMPv3 Explicit Host Tracking	Enabled

IGMP Snooping Configuration Guidelines and Restrictions

When configuring IGMP snooping, follow these guidelines and restrictions:

- To support Cisco Group Management Protocol (CGMP) client devices, configure the route processor (RP) as a CGMP server. See the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.2, "IP Multicast," "Configuring IP Multicast Routing," at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfmulti.html
- For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.
- IGMP snooping supports private VLANs. Private VLANs do not impose any restrictions on IGMP snooping.
- IGMP snooping constrains traffic in MAC multicast groups 0100.5e00.0001 to 0100.5eff.ffff.
- IGMP snooping does not constrain Layer 2 multicasts generated by routing protocols.

IGMP Snooping Querier Configuration Guidelines and Restrictions

When configuring the IGMP snooping querier, follow these guidelines and restrictions:

- Release 12.2(33)SXJ1 and later releases support redundant IGMP snooping queriers. To configure redundant IGMP snooping queriers, ensure that the tasks in the "Enabling IGMP Snooping" section on page 38-9 and "Configuring the IGMP Snooping Querier" section on page 38-10 are completed on more than one switch in the VLAN.

  When multiple IGMP snooping queriers are enabled in a VLAN, the querier with the lowest IP address in the VLAN is elected as the active IGMP snooping querier.

  An IGMP snooping querier election occurs if the active IGMP snooping querier goes down or if there is an IP address change on any of the queriers.

  Note To avoid unnecessary active querier time outs, configure the **ip igmp snooping querier query-interval** command with the same value on all queriers in a VLAN.

  Releases earlier than Release 12.2(33)SXJ1 do not support redundant IGMP snooping queriers. Enable the IGMP snooping querier on only one switch in the VLAN. (CSCsk48795)
- Configure the VLAN in global configuration mode (see Chapter 23, "Configuring VLANs").
- Configure an IP address on the VLAN interface (see Chapter 30, "Configuring Layer 3 Interfaces"). 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 does not start. The IGMP snooping querier disables itself if the IP address is cleared. When enabled, the IGMP snooping querier restarts if you configure an IP address.
- The IGMP snooping querier sends IGMPv3 querier messages. Although the IGMP version of the querier messages is not configurable, the querier is compatible with IGMPv2 hosts.
- When enabled, the IGMP snooping querier starts immediately. If IGMP traffic from a multicast router, or from another IGMP snooping querier in the VLAN, is detected after the IGMP snooping querier has started, the querier will disable itself.
- QoS does not support IGMP packets when IGMP snooping is enabled.

Configuring IGMP Snooping

Note To use IGMP snooping, configure a Layer 3 interface in the subnet for multicast routing (see Chapter 37, "Configuring IPv4 Multicast Layer 3 Switching") or enable the IGMP snooping querier in the subnet (see the "Configuring the IGMP Snooping Querier" section on page 38-10).

These sections describe how to configure IGMP snooping:

Note Except for the **ip igmp snooping** command, all IGMP snooping commands are supported only on VLAN interfaces.

Enabling IGMP Snooping

To enable IGMP snooping globally, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip igmp snooping`	Enables IGMP snooping.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show ip igmp interface vlan vlan_ID | include globally`	Verifies the configuration.

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

```
Router(config)# ip igmp snooping
Router(config)# end
Router# show ip igmp interface vlan 200 | include globally
```

```
  IGMP snooping is globally enabled
Router#
```

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

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping`	Enables IGMP snooping.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show ip igmp interface vlan vlan_ID | include snooping`	Verifies the configuration.

This example shows how to enable IGMP snooping on VLAN 25 and verify the configuration:

```
Router# interface vlan 25
Router(config-if)# ip igmp snooping
Router(config-if)# end
Router# show ip igmp interface vl25 | include snooping
IGMP snooping is globally enabled
  IGMP snooping CGMP-AutoDetect is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave (for v2) is disabled
  IGMP snooping querier is enabled. Querier is 11.1.22.252 (this system)
  IGMP snooping explicit-tracking is enabled
  IGMP snooping last member query response interval is 25000 ms
  IGMP snooping report-suppression is disabled
  IGMP snooping query interval is 60000 ms? New output
  IGMP snooping querier version is 3? New output
  IGMP snooping querier - TCN query count is 5? New output
  IGMP snooping querier - TCN query interval is 1000 ms
Router#
```

Configuring the IGMP Snooping Querier

Enabling the IGMP Snooping Querier

Use the IGMP snooping querier to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. To enable the IGMP snooping querier in a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects the VLAN interface.
Step 2	`Router(config-if)# ip address ip_address subnet_mask`	Configures the IP address and IP subnet.

	Command	Purpose
Step 3	`Router(config-if)# ip igmp snooping querier`	Enables the IGMP snooping querier.
Step 4	`Router(config-if)# end`	Exits configuration mode.
Step 5	`Router# show ip igmp interface vlan vlan_ID | include querier`	Verifies the configuration.

This example shows how to enable the IGMP snooping querier on VLAN 200 and verify the configuration:

```
Router# interface vlan 200
Router(config-if)# ip address 11.1.22.60 255.255.255.248
Router(config-if)# igmp snooping querier
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include Querier
IGMP snooping querier is enabled. Querier is 11.1.22.60 (this system)
```

Configuring the IGMP Snooping General Query Interval

In Release 12.2(33)SXJ1 and later releases, you can configure the interval for which the switch waits after sending a general query to determine if hosts are still interested in any multicast groups.

Note In releases earlier than Release 12.2(33)SXJ1, the general query interval is 60 seconds and is not configurable.

To configure the IGMP snooping general query interval, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping querier query-interval interval`	Configures the IGMP snooping general query interval. • Default value: 60000ms (60s). • The valid range is 1000 to 18000000 milliseconds. • With redundant IGMP snooping queriers, to avoid unnecessary active querier time outs, configure the same query-interval value on all queriers in a VLAN.

This example shows how to configure the IGMP snooping general query interval:

```
Router(config-if)# ip igmp snooping querier query-interval 60000
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include snooping query interval
  IGMP snooping query interval on this interface is 60000 ms
```

Configuring the IGMP Snooping TCN General Query Count

In Release 12.2(33)SXJ1 and later releases, you can configure the number of general queries that the IGMP snooping querier sends after receiving a topology change notification (TCN).

Note In releases earlier than Release 12.2(33)SXJ1, the TCN general query count is 1 and is not configurable.

To configure the TCN general query count, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping querier tcn query count count`	Configures the TCN general query count. • Default value: 2. • The valid range is 1 to 10 queries.

This example shows how to configure the TCN general query count:

```
Router(config-if)# ip igmp snooping querier tcn query count 2
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include TCN query count
  IGMP snooping querier - TCN query count is 2
```

Configuring the IGMP Snooping TCN General Query Interval

In Release 12.2(33)SXJ1 and later releases, you can configure the interval between general queries sent in response to TCNs.

Note In releases earlier than Release 12.2(33)SXJ1, the TCN general query interval is not applicable because the TCN general query count is 1 and is not configurable.

To configure the TCN general query interval, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping querier tcn query interval interval`	Configures the TCN general query interval. • Default value: 10000 ms (10s). • The valid range is 1000 to 255000 ms.

This example shows how to configure the TCN general query interval:

```
Router(config-if)# ip igmp snooping querier tcn query interval 10000
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include TCN query interval
  IGMP snooping querier - TCN query interval is 10000 ms
```

Configuring the IGMP Snooping Group-Specific Query Interval

You can configure the interval for which the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group.

Note When both IGMP fast-leave processing and the IGMP query interval are configured, fast-leave processing takes precedence.

To configure the IGMP snooping group-specific query interval, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping last-member-query-interval interval`	Configures the IGMP snooping group-specific query interval. • The default value is 1000 ms (1s). • In Release 12.2(33)SXJ1 and later releases, the valid range is 100 to 25500 milliseconds. • In releases earlier than Release 12.2(33)SXJ1, the valid range is 100 to 999 milliseconds.

This example shows how to configure the IGMP snooping query interval:

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include last
  IGMP snooping last member query interval on this interface is 200 ms
```

Enabling IGMP Fast-Leave Processing

Fast-leave configuration applies to IGMP version 2 hosts only. To enable IGMP fast-leave processing in a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping`	Enables IGMP snooping. This step is only necessary if IGMP snooping is not already enabled on this VLAN.
Step 3	`Router(config-if)# ip igmp snooping fast-leave`	Enables IGMP fast-leave processing in the VLAN.

This example shows how to enable IGMP fast-leave processing for IGMP version 2 hosts on the VLAN 200 interface, and how to verify the configuration:

```
Router# interface vlan 200
Router(config-if)# ip igmp snooping
Router(config-if)# ip igmp snooping fast-leave
Configuring fast leave on vlan 200
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include fast-leave
IGMP snooping fast-leave is enabled on this interface
```

Configuring Source-Specific Multicast Mapping

Note Do not configure SSM mapping in a VLAN that supports IGMPv3 multicast receivers.

To configure source-specific multicast (SSM) mapping, see this publication:

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_basic_cfg.html#SSM_Overview

CGMP Automatic Detection

By default, the switch will detect Cisco group management protocol (CGMP) packets using the CGMP automatic detection feature. CGMP automatic detection operates as follows:

- When CGMP traffic is detected on a VLAN, IGMP report suppression is disabled on that VLAN for a period of five minutes.
- Any new CGMP traffic on the VLAN will begin a new five-minute period.
- When no new CGMP traffic has been detected on the VLAN for five minutes, the IGMP report suppression will revert to the configured status.

The CGMP automatic detection feature has no access to VTP information and causes the switch to send CGMP traffic to VLANs that VTP has pruned from trunks. To avoid this situation, you can disable the CGMP automatic detection feature by entering the **no ip igmp snooping cgmp auto-detect** global configuration command. Disabling CGMP automatic detection restricts CGMP traffic to Layer 2. When CGMP automatic detection is disabled, IGMP report suppression must be disabled manually for any VLAN that will use CGMP.

To disable CGMP automatic detection, perform this task:

	Command	Purpose
Step 1	`Router(config)# no ip igmp snooping cgmp auto-detect`	Disables the CGMP auto-detect mode globally.
Step 2	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 3	`Router(config-if)# no ip igmp snooping report-suppression`	Disables IGMP snooping report suppression so that CGMP receives all the report messages on this VLAN.
Step 4	`Router(config-if)# ip cgmp`	Enables CGMP mode on this VLAN.

Configuring IGMPv3 Explicit Host Tracking

To enable explicit host tracking on a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp explicit-tracking`	Enables explicit host tracking.
Step 3	`Router# show ip igmp snooping explicit-tracking {vlan vlan-id}`	Displays information about the explicit host tracking status for IGMPv3 hosts.

This example shows how to enable explicit host tracking:

```
Router(config)# interface vlan 25
Router(config-if)# ip igmp explicit-tracking
Router(config-if)# end
```

This example shows how to display information about explicit host tracking:

```
Router# show ip igmp snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
--------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
```

This example shows the information displayed for VPLS interfaces:

```
Router# show ip igmp snooping explicit-tracking vlan 25
Source/Group                    Interface      Reporter      Filter_mode
--------------------------------------------------------------------------
10.1.1.1/224.1.1.1              Vl25:VPLS3/62   2.2.2.1       INCLUDE
10.2.2.2/224.2.2.1              Vl25:A-VPLS14/0 2.2.2.2       INCLUDE
```

Displaying IGMP Snooping Information

These sections describe displaying IGMP snooping information:

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
`Router# show ip igmp snooping mrouter vlan_ID`	Displays multicast router interfaces.

This example shows how to display the multicast router interfaces in VLAN 3:

```
Router# show ip igmp snooping mrouter vlan 3
vlan            ports
-----+---------------------------------------
   3  Router,VPLS3/62,A-VPLS14/0
Router#
```

Displaying MAC Address Multicast Entries

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

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

This example shows how to display MAC address multicast entries for VLAN 3:

```
Router# show mac-address-table multicast vlan 3
vlan   mac address     type   learn qos             ports
-----+---------------+--------+-----+---+--------------------------------
   3  0100.5e01.0101    static  Yes          -   Router,VPLS 2.2.2.2,A-VPLS 7.7.7.7
   3  0100.5e02.0201    static  Yes          -   Router,VPLS 2.2.2.2,A-VPLS 7.7.7.7
Router#
```

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

```
Router# show mac-address-table multicast 3 count

Multicast MAC Entries for vlan 3:    2
Router#
```

Displaying IGMP Snooping Information for a VLAN Interface

Note When you apply the **ip igmp snooping** command and associated commands on any VLAN interface, the commands continue to function even if the VLAN interface is in shutdown state.

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

Command	Purpose
Router# **show ip igmp interface** *vlan_ID*	Displays IGMP snooping information on a VLAN interface.

This example shows how to display IGMP snooping information on the VLAN 200 interface:

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
  Internet address is 43.0.0.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
```

```
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity:1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 43.0.0.1 (this system)
  IGMP querying router is 43.0.0.1 (this system)
  Multicast groups joined by this system (number of users):
      224.0.1.40(1)
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave is disabled and querier is disabled
  IGMP snooping explicit-tracking is enabled on this interface
  IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

Displaying IGMP Snooping Statistics

The **show ip igmp snooping statistics interface** *vlan_ID* command displays the following information:

- The list of ports that are members of a group
- The filter mode
- The reporter-address behind the port
- The last-join and last-leave information collected since the last time a **clear ip igmp snooping statistics** command was entered

To display IGMP snooping statistics, perform this task:

Command	Purpose
`Router#` **`show ip igmp snooping statistics interface`** *`vlan_ID`*	Displays IGMP snooping information on a VLAN interface.

This example shows IGMP snooping statistics information for interface VLAN 25:

```
Router# show ip igmp snooping statistics interface vlan 25

Snooping statistics for Vlan25
#channels: 2
#hosts   : 2
Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/224.1.1.1      Vl25:VPLS3/62    2.2.2.1       00:01:47      00:00:51      -
10.2.2.2/224.2.2.1      Vl25:A-VPLS14/0  2.2.2.2       00:01:50      00:00:52      -
Router#
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum