



## CHAPTER 30

# Configuring IGMP Snooping for IPv4 Multicast Traffic

---

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping for IPv4 multicast traffic on the Cisco 7600 series routers.



### Note

- For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:  
[http://www.cisco.com/en/US/products/hw/routers/ps368/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html)
  - To constrain IPv6 Multicast traffic, see [Chapter 29, “Configuring MLDv2 Snooping for IPv6 Multicast Traffic.”](#)
- 

This chapter consists of these sections:

- [Understanding How IGMP Snooping Works, page 30-1](#)
- [Default IGMP Snooping Configuration, page 30-7](#)
- [IGMP Snooping Configuration Guidelines and Restrictions, page 30-8](#)
- [IGMP Snooping Querier Configuration Guidelines and Restrictions, page 30-8](#)
- [Enabling the IGMP Snooping Querier, page 30-9](#)
- [Configuring IGMP Snooping, page 30-9](#)

## Understanding How IGMP Snooping Works

These sections describe IGMP snooping:

- [IGMP Snooping Overview, page 30-2](#)
- [Joining a Multicast Group, page 30-2](#)
- [Leaving a Multicast Group, page 30-4](#)
- [Understanding the IGMP Snooping Querier, page 30-5](#)
- [Understanding IGMP Version 3 Support, page 30-5](#)

## IGMP Snooping Overview

You can configure the router 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.

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 28, “Configuring IPv4 Multicast Layer 3 Switching.”](#)

You can configure the IGMP snooping querier on the router to support IGMP snooping in subnets that do not have any multicast router interfaces. For more information about the IGMP snooping querier, see the [“Enabling the IGMP Snooping Querier” section on page 30-9.](#)

IGMP (on a multicast router) or the IGMP snooping querier (on the supervisor engine) sends out periodic general IGMP queries that the router 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 router forwards general queries from multicast routers to all ports in a VLAN).

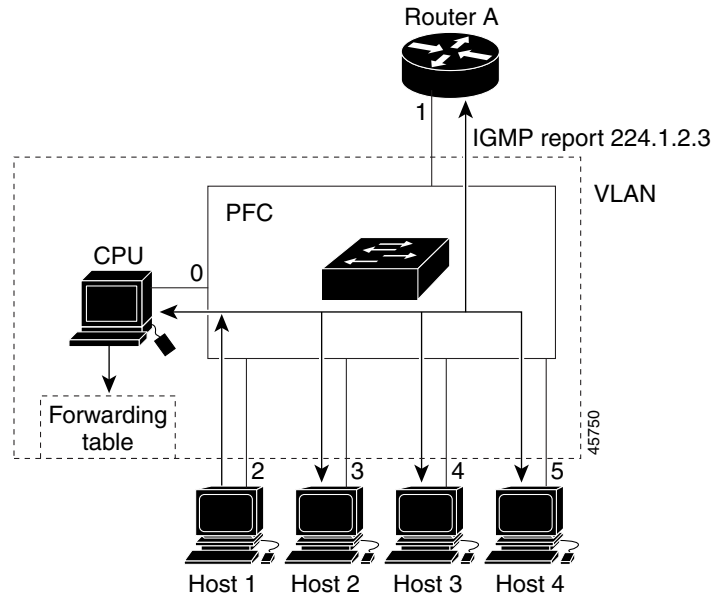
In response to an IGMP join request, the router creates an entry in its Layer 2 forwarding table for the VLAN on which the join request was received. When other hosts that are interested in this multicast traffic send IGMP join requests, the router adds them to the existing Layer 2 forwarding table entry. The router 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 router forwards multicast traffic for the multicast group specified in the join message to the interfaces where join messages were received (see [Figure 30-1](#)).

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 30-1 Initial IGMP Join Message



Multicast router A sends a general query to the router, 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 30-1, that includes the port numbers of Host 1, the multicast router, and the router internal CPU.

Table 30-1 IGMP Snooping Forwarding Table

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

The router 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 30-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 30-2. 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 30-2 Second Host Joining a Multicast Group

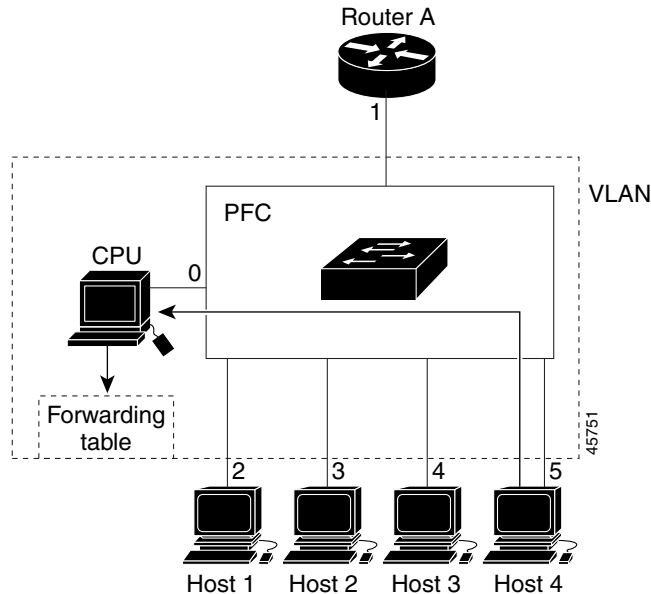


Table 30-2 Updated IGMP Snooping Forwarding Table

| 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 30-4](#)
- [Fast-Leave Processing, page 30-5](#)

### 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 router waits before updating the table entry is called the “last member query interval.” To configure the interval, enter the **ip igmp snooping last-member-query-interval** *interval* command.

## 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 router 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 router that wants to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

You can enable the IGMP snooping querier on all the Cisco 7600 series routers in the VLAN, but for each VLAN that is connected to switches that use IGMP to report interest in IP multicast traffic, you must configure at least one router as the IGMP snooping querier.

You can configure a router to generate IGMP queries on a VLAN regardless of whether or not IP multicast routing is enabled.

## Understanding IGMP Version 3 Support

These sections describe IGMP version 3 support:

- [IGMP Version 3 Support Overview, page 30-6](#)
- [IGMPv3 Fast-Leave Processing, page 30-6](#)
- [Proxy Reporting, page 30-6](#)
- [Explicit Host Tracking, page 30-7](#)

## IGMP Version 3 Support Overview

IGMP snooping supports IGMP version 3. IGMP version 3 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 IGMP version 3 snooping on a Cisco 7600 series router, the system maintains IGMP version 3 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 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.

## IGMPv3 Fast-Leave Processing

IGMP version 3 fast-leave processing is enabled by default. To disable IGMP version 3 fast-leave processing you must turn off explicit-host tracking.

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 enabled, 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 router 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 router 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 router 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 are 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 router 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 30-3 shows the default IGMP snooping configuration.

**Table 30-3** 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  |
| IGMPv3 Explicit Host Tracking        | Enabled   |
| IGMPv3 SSM Safe Reporting            | Disabled  |

# 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 Multilayer Switch Feature Card (MSFC) as a CGMP server. Refer to 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/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt3/1cfmulti.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfmulti.htm)
- For more information on IP multicast and IGMP, refer to 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:

- Configure the VLAN in global configuration mode (see [Chapter 14, “Configuring VLANs”](#)).
- Configure an IP address on the VLAN interface (see [Chapter 21, “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 supports IGMP version 2.
- When enabled, the IGMP snooping querier does not start if it detects IGMP traffic from a multicast router.
- When enabled, the IGMP snooping querier starts after 60 seconds with no IGMP traffic detected from a multicast router.
- When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.
- QoS does not support IGMP packets when IGMP snooping is enabled.
- You can enable the IGMP snooping querier on all the Cisco 7600 series routers in the VLAN. One router is elected as the querier.

**Note**

When you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.

## 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)# <b>interface vlan</b> <i>vlan_ID</i>                               | Selects the VLAN interface.              |
| Step 2 | Router(config-if)# <b>ip address</b> <i>ip_address</i> <i>subnet_mask</i>          | Configures the IP address and IP subnet. |
| Step 3 | Router(config-if)# <b>ip igmp snooping querier</b>                                 | Enables the IGMP snooping querier.       |
|        | Router(config-if)# <b>no ip igmp snooping querier</b>                              | Disables the IGMP snooping querier.      |
| Step 4 | Router(config-if)# <b>end</b>  | Exits configuration mode.                |
| Step 5 | Router# <b>show ip igmp interface vlan</b> <i>vlan_ID</i>   <b>include querier</b> | 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 172.20.52.106 255.255.255.248
Router(config-if)# igmp snooping querier
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include querier
IGMP snooping querier is enabled on this interface
Router#
```

## Configuring IGMP Snooping



### Note

To use IGMP snooping, configure a Layer 3 interface in the subnet for multicast routing (see [Chapter 28, “Configuring IPv4 Multicast Layer 3 Switching”](#)) or enable the IGMP snooping querier in the subnet (see the [“Enabling the IGMP Snooping Querier”](#) section on page 30-9).

IGMP snooping allows Cisco 7600 series routers to examine IGMP packets and make forwarding decisions based on their content.

These sections describe how to configure IGMP snooping:

- [Enabling IGMP Snooping, page 30-10](#)
- [Configuring a Static Connection to a Multicast Receiver, page 30-11](#)
- [Configuring a Multicast Router Port Statically, page 30-11](#)
- [Configuring the IGMP Snooping Query Interval, page 30-11](#)
- [Enabling IGMP Fast-Leave Processing, page 30-12](#)
- [Configuring Source Specific Multicast \(SSM\) Mapping, page 30-12](#)
- [Enabling SSM Safe Reporting, page 30-13](#)

- [Configuring IGMPv3 Explicit Host Tracking, page 30-13](#)
- [Displaying IGMP Snooping Information, page 30-14](#)

**Note**

Except for the global enable command, all IGMP snooping commands are supported only on VLAN interfaces.

## Enabling IGMP Snooping

To enable IGMP snooping globally, perform this task:

|               | Command  | Purpose                     |
|---------------|--|-----------------------------|
| <b>Step 1</b> | Router(config)# <b>ip igmp snooping</b>                                      | Enables IGMP snooping.      |
|               | Router(config)# <b>no ip igmp snooping</b>                                   | Disables IGMP snooping.     |
| <b>Step 2</b> | Router(config)# <b>end</b>   | Exits configuration mode.   |
| <b>Step 3</b> | Router# <b>show ip igmp interface vlan <i>vlan_ID</i>   include globally</b> | 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                     |
|---------------|--|-----------------------------|
| <b>Step 1</b> | Router(config)# <b>interface vlan <i>vlan_ID</i></b>                         | Selects a VLAN interface.   |
| <b>Step 2</b> | Router(config-if)# <b>ip igmp snooping</b>                                   | Enables IGMP snooping.      |
|               | Router(config-if)# <b>no ip igmp snooping</b>                                | Disables IGMP snooping.     |
| <b>Step 3</b> | Router(config-if)# <b>end</b>  | Exits configuration mode.   |
| <b>Step 4</b> | Router# <b>show ip igmp interface vlan <i>vlan_ID</i>   include snooping</b> | 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 v125 | include snooping
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#
```

## Configuring a Static Connection to a Multicast Receiver

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

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | Router(config)# <b>mac-address-table static</b> <i>mac_addr</i><br><b>vlan</b> <i>vlan_id</i> <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i><br>[ <b>disable-snooping</b> ] | Configures a static connection to a multicast receiver. |
|        | Router(config)# <b>no mac-address-table static</b><br><i>mac_addr</i> <b>vlan</b> <i>vlan_id</i>  | Clears a static connection to a multicast receiver.     |
| Step 2 | Router(config-if)# <b>end</b>   | Exits configuration mode.                               |
| Step 3 | Router# <b>show mac-address-table address</b> <i>mac_addr</i>   | Verifies the configuration.                             |

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

When you configure a static connection, enter the **disable-snooping** keyword to prevent multicast traffic addressed to the statically configured multicast MAC address from also being sent to other ports in the same VLAN.

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

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 interface fastethernet 5/7
```

## Configuring a Multicast Router Port Statically

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

|        | Command  | Purpose   |
|--------|--|---|
| Step 1 | Router(config-if)# <b>ip igmp snooping mrouter</b><br><b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i> | Configures a static connection to a multicast router. |
| Step 2 | Router(config-if)# <b>end</b>  | Exits configuration mode.                             |
| Step 3 | Router# <b>show ip igmp snooping mrouter</b>   | Verifies the configuration.                           |

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

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

```
Router(config-if)# ip igmp snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

## Configuring the IGMP Snooping Query Interval

You can configure the interval for which the router 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 interval for the IGMP snooping queries sent by the router, perform this task:

|        | Command   | Purpose  |
|--------|---|--|
| Step 1 | Router(config)# <b>interface vlan</b> <i>vlan_ID</i>                                  | Selects a VLAN interface.  |
| Step 2 | Router(config-if)# <b>ip igmp snooping last-member-query-interval</b> <i>interval</i> | Configures the interval for the IGMP snooping queries sent by the router. Default is 1 second. Valid range is 100 to 999 milliseconds. |
|        | Router(config-if)# <b>no ip igmp snooping last</b>                                    | Reverts to the default value.  |

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

To enable IGMP fast-leave processing in a VLAN, perform this task:

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | Router(config)# <b>interface vlan</b> <i>vlan_ID</i>     | Selects a VLAN interface.                        |
| Step 2 | Router(config-if)# <b>ip igmp snooping fast-leave</b>    | Enables IGMP fast-leave processing in the VLAN.  |
|        | Router(config-if)# <b>no ip igmp snooping fast-leave</b> | Disables IGMP fast-leave processing in the VLAN. |

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

```
Router# interface vlan 200
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
Router(config-if)#
```

## Configuring Source Specific Multicast (SSM) Mapping



### Note

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

To configure SSM mapping, refer to this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gtssmma.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtssmma.htm)

## Enabling SSM Safe Reporting


**Note**

Source-specific multicast (SSM) safe reporting is presently deprecated.

When you configure SSM safe reporting, the group mode is IGMPv3 even in the presence of IGMPv1 and IGMPv2 hosts.

To make sure the router is able to support both IGMPv1, IGMPv2, and IGMPv3 hosts in the same VLAN, perform this task:

|               | Command  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | Router(config)# <b>interface vlan</b> <i>vlan_ID</i>             | Selects a VLAN interface.                         |
| <b>Step 2</b> | Router(config-if)# <b>ip igmp snooping ssm-safe-reporting</b>    | Enables support for both IGMPv2 and IGMPv3 hosts. |
|               | Router(config-if)# <b>no ip igmp snooping ssm-safe-reporting</b> | Clears the configuration.                         |

This example shows how to configure the router to support both IGMPv2 and IGMPv3 hosts:

```
Router(config)# interface vlan 10
Router(config-if)# ip igmp snooping ssm-safe-reporting
```

## Configuring IGMPv3 Explicit Host Tracking

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

|               | Command   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | Router(config)# <b>interface vlan</b> <i>vlan_ID</i>                  | Selects a VLAN interface.  |
| <b>Step 2</b> | Router(config-if)# <b>ip igmp snooping explicit-tracking</b>          | Enables explicit host tracking.  |
|               | Router(config-if)# <b>no ip igmp snooping explicit-tracking</b>       | Clears the explicit host tracking configuration.                               |
| <b>Step 3</b> | Router# <b>show ip igmp snooping explicit-tracking {vlan vlan-id}</b> | 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 snooping explicit-tracking
Router(config-if)# end
Router# show ip igmp snooping explicit-tracking vlan 25
```

| Source/Group       | Interface | Reporter  | Filter_mode |
|--------------------|-----------|-----------|-------------|
| 10.1.1.1/226.2.2.2 | V125:1/2  | 16.27.2.3 | INCLUDE     |
| 10.2.2.2/226.2.2.2 | V125:1/2  | 16.27.2.3 | INCLUDE     |

## Displaying IGMP Snooping Information

These sections describe displaying IGMP snooping information:

- [Displaying Multicast Router Interfaces](#), page 30-14
- [Displaying MAC Address Multicast Entries](#), page 30-14
- [Displaying IGMP Snooping Information for a VLAN Interface](#), page 30-15
- [Displaying IGMP Snooping Statistics](#), page 30-15

### Displaying Multicast Router Interfaces

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

To display multicast router interfaces, perform this task:

| Command  | Purpose                               |
|--|---------------------------------------|
| Router# <b>show ip igmp snooping mrouter</b><br><i>vlan_ID</i> | Displays multicast router interfaces. |

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

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

### Displaying MAC Address Multicast Entries

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

| Command  | Purpose  |
|--|--|
| Router# <b>show mac-address-table multicast</b> <i>vlan_ID</i><br>[ <i>count</i> ] | Displays MAC address multicast entries for a VLAN. |

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

```
Router# show mac-address-table multicast vlan 1
vlan  mac address      type    qos      ports
-----+-----+-----+-----+-----
 1    0100.5e02.0203    static  --    Gi1/1,Gi2/1,Fa3/48,Router
 1    0100.5e00.0127    static  --    Gi1/1,Gi2/1,Fa3/48,Router
 1    0100.5e00.0128    static  --    Gi1/1,Gi2/1,Fa3/48,Router
 1    0100.5e00.0001    static  --    Gi1/1,Gi2/1,Fa3/48,Router,Switch
Router#
```

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

```
Router# show mac-address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

## Displaying IGMP Snooping Information for a VLAN Interface

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

| Command  | Purpose   |
|--|---|
| Router# <b>show ip igmp interface</b> <i>vlan_ID</i> | 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# <b>show ip igmp snooping statistics interface</b> <i>vlan_ID</i> | 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 :1
```

| Source/Group       | Interface  | Reporter  | Uptime   | Last-Join | Last-Leave |
|--------------------|------------|-----------|----------|-----------|------------|
| 10.1.1.1/226.2.2.2 | Gi1/2:V125 | 16.27.2.3 | 00:01:47 | 00:00:50  | -          |
| 10.2.2.2/226.2.2.2 | Gi1/2:V125 | 16.27.2.3 | 00:01:47 | 00:00:50  | -          |

```
Router#
```