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
- 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).

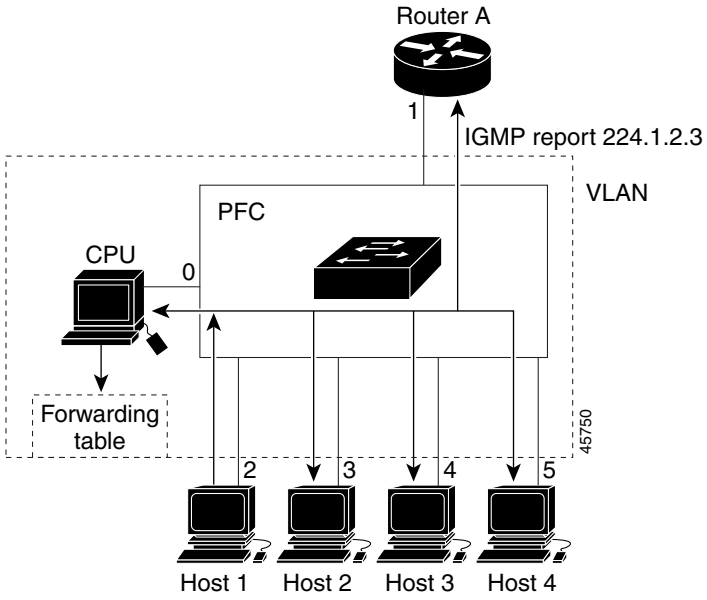
In response to an IGMP join request, the router creates an entry in its Layer 2 forwarding table for the VLAN on which the join request was received. When other hosts that are interested in this multicast traffic send IGMP join requests, the router adds them to the existing Layer 2 forwarding table entry. 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

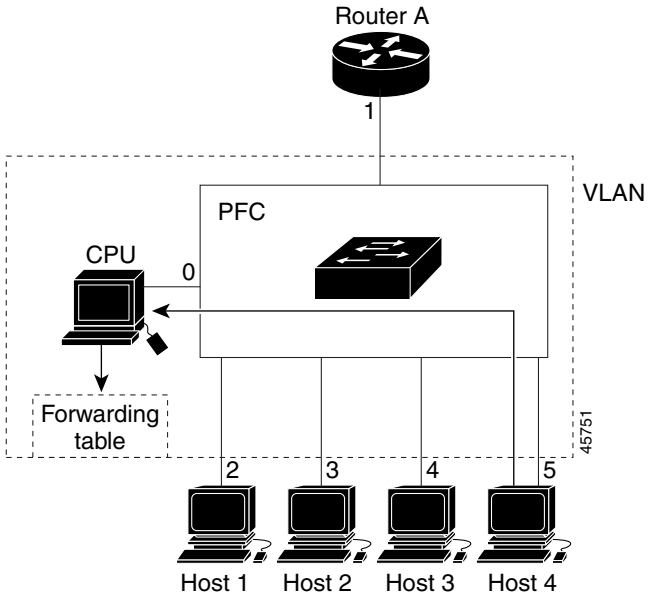


Table 30-2 Updated IGMP Snooping Forwarding Table

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 recieves 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 recieves 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
- 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)# 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.
Step 3	`Router(config-if)# ip igmp snooping querier` `Router(config-if)# no ip igmp snooping querier`	Enables the IGMP snooping querier. Disables 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 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
Step 1	`Router(config)# ip igmp snooping`	Enables IGMP snooping.
	`Router(config)# no ip igmp snooping`	Disables 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.
	`Router(config-if)# no ip igmp snooping`	Disables 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 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)# mac-address-table static` *mac_addr* `vlan` *vlan_id* `interface` *type*[1] *slot/port* [`disable-snooping`]	Configures a static connection to a multicast receiver.
	`Router(config)# no mac-address-table static` *mac_addr* `vlan` *vlan_id*	Clears a static connection to a multicast receiver.
Step 2	`Router(config-if)# end`	Exits configuration mode.
Step 3	`Router# show mac-address-table address` *mac_addr*	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)# ip igmp snooping mrouter interface` *type*[1] *slot/port*	Configures a static connection to a multicast router.
Step 2	`Router(config-if)# end`	Exits configuration mode.
Step 3	`Router# show ip igmp snooping mrouter`	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)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping last-member-query-interval interval`	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)# no ip igmp snooping last`	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)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping fast-leave`	Enables IGMP fast-leave processing in the VLAN.
	`Router(config-if)# no ip igmp snooping fast-leave`	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

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
Step 1	`Router(config)# interface vlan` *vlan_ID*	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping ssm-safe-reporting`	Enables support for both IGMPv2 and IGMPv3 hosts.
	`Router(config-if)# no ip igmp snooping ssm-safe-reporting`	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
Step 1	`Router(config)# interface vlan` *vlan_ID*	Selects a VLAN interface.
Step 2	`Router(config-if)# ip igmp snooping explicit-tracking`	Enables explicit host tracking.
	`Router(config-if)# no ip igmp snooping explicit-tracking`	Clears the explicit host tracking configuration.
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 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              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     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# **show ip igmp snooping mrouter** *vlan_ID*	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# **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 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# **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   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50      -
Router#
```

Troubleshooting

This section describes how to troubleshoot common IGMP issues.

Scenarios/Problems	Solution
How do I verify whether the multicast queries are sent and reports are received from the host?	Queries are generated by the IGMP PI code and forwarded through interfaces. Use the PI group specific **debug ip igmp grp**,**debug mmls igmp-even**t, and **debug mmls igmp-pak** commands.

How do I verify the IGMP membership of the node?	Use the **show ip igmp vrf 0 groups 0** command. This example shows a sample output from the command:
	`csc76d#show ip igmp vrf blue groups 226.6.6.6`
	`IGMP Connected Group Membership`
	`Group Address Interface Uptime Expires Last Reporter Group Accounted`
	`226.6.6.6 GigabitEthernet4/0/3 00:15:32 00:02:42 200.3.3.202`
	`csc76d#`

How do I know the properties of the IGMP interface?	Use the **show ip igmp vrf 0 interface** command. The command will tell you whether it is a Querier/DR and the timer values for each interface. This example shows a sample output from this command:
	`csc76d#show ip igmp vrf blue interface gi 4/0/3`
	`GigabitEthernet4/0/3 is up, line protocol is up`
	`Internet address is 200.3.3.3/24`
	`IGMP is enabled on interface`
	`Multicast Routing table blue`
	`Current IGMP host version is 2`
	`Current IGMP router version is 2`
	`IGMP query interval is 60 seconds`
	`IGMP configured query interval is 60 seconds`
	`IGMP querier timeout is 120 seconds`
	`IGMP configured 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 200.3.3.3 (this system)`
	`IGMP querying router is 200.3.3.2`
	`No multicast groups joined by this system`
	`csc76d#`

Scenarios/Problems	Solution

How do I verify that the IGMP packets are coming into the PI code?	Use the **debug ip igmp vrf 0 0** command to verify whether the IGMP packets are coming into the PI code. The following example shows a sample output of this command:
	`*Oct 6 11:31:40.263: IGMP(1): Received v2 Report on GigabitEthernet3/5 from 200.3.3.202 for 226.6.6.6`
	`*Oct 6 11:31:40.263: IGMP(1): Received Group record for group 226.6.6.6, mode 2 from 200.3.3.202 for 0 sources`
	`*Oct 6 11:31:40.263: IGMP(1): Updating EXCLUDE group timer for 226.6.6.6`
	`*Oct 6 11:31:40.263: IGMP(1): MRT Add/Update GigabitEthernet3/5 for (*,226.6.6.6) by 0`

How do I verify that the packets have reached the switch processor?	Use the **debug platform software multicast igmp event** and **debug platform software multicast igmp pak** commands to verify whether the packets have reached the switch processor. The following example shows the debug output:
	Note This command is introduced in 12.2(SRE) release. It may not work in old releases.
	`csc76b#show vlan internal usage | i 1025`
	`1025 GigabitEthernet3/5`
	`csc76b#`
	`*Oct 6 11:31:40.259: SP: RELAYED PAK to index 0x00084401, vlan 1025`
	`*Oct 6 11:31:40.259: SP: Packet dump:`
	`18000070: 0100 5E060606 00097B04 ..^.....{.Z>`
	`HdL`
	`18000080: E4700800 45C0001C 018E0000 010203B9 dp..E@.........9Z>`
	`HdL`
	`18000090: C80303CA E2060606 160001F3 E2060606 H..Jb......sb...Z>`
	`HdL`
	`180000A0: 00000000 00000000 00000000 00000000 ................Z>`
	`HdL`
	`180000B0: 000018 ... Z>`
	`HdL`

How do I check the multicast groups with receivers that are directly connected to the router and that were learned through IGMP?	Use the **show ip igmp groups** command. This is a sample output from the command with the **group-address** argument and **detail** keyword:
	`Router# show ip igmp groups 192.168.1.1 detail`
	`Interface:  Ethernet3/2`
	`Group:  192.168.1.1`
	`Uptime:  01:58:28`
	`Group mode:  INCLUDE`
	`Last reporter:  10.0.119.133`
	`CSR Grp Exp:  00:02:38`
	`Group source list: (C - Cisco Src Report, U - URD, R - Remote S-Static, M - SSM Mapping)`
	`Source Address  Uptime  v3 Exp  CSR Exp  Fwd  Flags`
	`172.16.214.1  01:58:28  stopped  00:02:31  Yes  C`

Scenarios/Problems	Solution

How do I verify whether the incoming interface and output interfaces are proper?	To verify that the incoming interface and output interfaces are proper, follow these steps:
	• Use the **show ip mroute** command to display the MRIB information. Check the incoming interface and outgoing interface list. If this information is correct then the Mroute information is correct. If it is incorrect, then enable the **debug ip mrouting** command. This output is from the **debug ip mrouting** command:
	`13.0.0.1, 228.1.1.1), 04:02:28/00:03:19, flags: FT`
	`Incoming interface: GigabitEthernet4/0/0, RPF nbr 0.0.0.0`
	`Outgoing interface list:`
	`FastEthernet1/11, Forward/Sparse, 03:33:01/00:02:59`
	`TenGigabitEthernet2/0/0, Forward/Sparse, 03:38:23/00:03:29`
	• Use the **show ip mrib route** command to display the MRIB information with MRIB flags. Look at the flags. See whether the **A** Flag is against the accept interface and the **F Flag** is against the forwarding interface. This should match with the above output of **show ip mroute** command. If it is incorrect, then enable **debug ip mrib command**. This output is from the **debug ip mrib** command:
	`(13.0.0.1,228.1.1.1) RPF nbr: 0.0.0.0 Flags: K DDE`
	`GigabitEthernet4/0/0 Flags: A`
	`FastEthernet1/11 Flags: F NS`
	`TenGigabitEthernet2/0/0 Flags: F NS`
	• Check the output of the **show ip mfib** command. Check if the information is correct by looking at the **A Flag** against the accept interface and the **F Flag** against the forwarding interface. This should match with the output of **show ip mrib route** command. If it is not correct then enable **debug ip mfib** command. This is a sample output:

Scenarios/Problems	Solution
	(13.0.0.1,228.1.1.1) Flags: K HW DDE Platform Flags: HW Slot 5: HW Forwarding: 0/0, Platform Flags: HF Slot 4: HW Forwarding: 70515/104503230, Platform Flags: HF Slot 2: HW Forwarding: 0/0, Platform Flags: HF Slot 1: HW Forwarding: 0/0, Platform Flags: HF SW Forwarding: 1/0/1482/0, Other: 84/0/84 HW Forwarding: 70515/5/1482/57, Other: 0/0/0 GigabitEthernet4/0/0 Flags: RA A Platform Flags: FastEthernet1/11 Flags: RF F NS Platform Flags: HW CEF: Adjacency with MAC: 01005E01010100152BE0AEC00800 Pkts: 0/0 TenGigabitEthernet2/0/0 Flags: RF F NS Platform Flags: HW CEF: Adjacency with MAC: 01005E01010100152BE0AEC00800 Pkts:0/0 • Check the output of the **show ip rpf** command. Compare the output with the source address of the stream and ensure that it is same as the one pointed by the incoming interface in MROUTE, MRIB and MFIB outputs above. 7606-3#sh ip rpf 13.0.0.1 RPF information for ? (13.0.0.1) RPF interface: GigabitEthernet4/0/0 <<<<<<<<<<<<<<<<<<<< RPF neighbor: ? (13.0.0.1) - directly connected RPF route/mask: 13.0.0.0/8 RPF type: multicast (connected) Doing distance-preferred lookups across tables RPF topology: ipv4 multicast base 7606-3#
How do I display information about PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages?	Use the **show ip pim neighbor** command in user EXEC or privileged EXEC mode. This example shows output from the command: Router# **show ip pim neighbor** PIM Neighbor Table Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority, S - State Refresh Capable Neighbor Interface Uptime/Expires Ver DR Address Prio/Mode 10.0.0.1 GigabitEthernet10/2 00:01:29/00:01:15 v2 1 / S 10.0.0.3 GigabitEthernet10

Scenarios/Problems	Solution

How do I know the active rendezvous points (RPs) that are cached with associated multicast routing entries?	Use the **show ip pim rp** command in user EXEC or privileged EXEC mode. This is a sample output from the command:
	`Router# show ip pim rp`
	`Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48`
	
	This is a sample output from the **show ip pim rp command** when the **mapping** keyword is specified:
	`Router# show ip pim rp mapping`
	`PIM Group-to-RP Mappings`
	`This system is an RP (Auto-RP)`
	`This system is an RP-mapping agent`
	`Group(s) 227.0.0.0/8`
	`  RP 10.10.0.2 (?), v2v1, bidir`
	`    Info source:10.10.0.2 (?), via Auto-RP`
	`         Uptime:00:01:42, expires:00:00:32`
	`Group(s) 228.0.0.0/8`
	`  RP 10.10.0.3 (?), v2v1, bidir`
	`    Info source:10.10.0.3 (?), via Auto-RP`
	`         Uptime:00:01:26, expires:00:00:34`
	`Group(s) 229.0.0.0/8`
	`  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir`
	`    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP`
	`         Uptime:00:00:52, expires:00:00:37`
	`Group(s) (-)230.0.0.0/8`
	`  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir`
	`    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP`
	`         Uptime:00:00:52, expires:00:00:37`
	
	This is a sample output from the **show ip pim rp command** when the **metric** keyword is specified:
	`Router# show ip pim rp metric`
	`RP Address  Metric Pref  Metric  Flags  RPF Type Interface`
	`10.10.0.2  0  0  L  unicast Loopback0`
	`10.10.0.3  90  409600  L  unicast Ethernet3/3`
	`10.10.0.5  90  435200  L  unicast Ethernet3/3`

Scenarios/Problems	Solution

How do I know information about interfaces configured for PIM?	Use the **show ip pim interface** command in user EXEC or privileged EXEC mode. This is a sample output from the command:
	
	`Router# show ip pim interface`
	`Address Interface Ver/ Nbr Query DR`
	`DR`
	`Mode Count Intvl`
	`Prior`
	`10.1.0.1 GigabitEthernet0/0 v2/SD 0 30 1`
	`10.1.0.1`
	`10.6.0.1 GigabitEthernet0/1 v2/SD 1 30 1`
	`10.6.0.2`
	`10.2.0.1 ATM1/0.1 v2/SD 1 30 1`
	`0.0.0.0`
	
	This is a sample output from the **show ip pim interface** command when an interface is specified:
	
	`Router# show ip pim interface Ethernet1/0`
	`Address Interface Ver/ Nbr Query DR`
	`DR`
	`Mode Count Intvl`
	`Prior`
	`172.16.1.4 Ethernet1/0 v2/S 1 100 ms 1`
	`172.16.1.4`
	
	This is a sample output from the **show ip pim interface** command when the **count** keyword is specified:
	
	`Router# show ip pim interface count`
	`Address Interface FS Mpackets In/Out`
	`172.16.121.35 Ethernet0 * 548305239/13744856`
	`172.16.121.35 Serial0.33 * 8256/67052912`
	`192.168.12.73 Serial0.1719 * 219444/862191`
	
	This is a sample output from the **show ip pim interface** command when the **count** keyword is specified and IP MMLS is enabled. The example lists the PIM interfaces that are fast switched and process switched, and the packet counts for these interfaces. The H flag is added to interfaces where IP MMLS is enabled.

Scenarios/Problems	Solution

```
Router# show ip pim interface count
States: FS - Fast Switched, H - Hardware Switched
Address          Interface          FS  Mpackets In/Out
192.168.10.2       Vlan10             * H 40886/0
192.168.11.2       Vlan11             * H 0/40554
192.168.12.2       Vlan12             * H 0/40554
192.168.23.2       Vlan23             *   0/0
192.168.24.2       Vlan24             *   0/0
```

These are two sample outputs from the **show ip pim interface** command when the **df** keyword is specified:

```
Router# show ip pim interface df
Interface          RP               DF Winner        Metric
Uptime
Ethernet3/3        10.10.0.2        10.4.0.2         0
00:03:49
                   10.10.0.3        10.4.0.3         0
00:01:49
                   10.10.0.5        10.4.0.4         409600
00:01:49
Ethernet3/4        10.10.0.2        10.5.0.2         0
00:03:49
                   10.10.0.3        10.5.0.2         409600
00:02:32
                   10.10.0.5        10.5.0.2         435200
00:02:16
Loopback0          10.10.0.2        10.10.0.2        0
00:03:49
                   10.10.0.3        10.10.0.2        409600
00:02:32
                   10.10.0.5        10.10.0.2        435200
00:02:16
Router# show ip pim interface Ethernet3/3 df 10.10.0.3
Designated Forwarder election for Ethernet3/3, 10.4.0.2, RP
10.10.0.3
  State                           Non-DF
  Offer count is                  0
  Current DF ip address           10.4.0.3
  DF winner up time               00:02:33
  Last winner metric preference   0
  Last winner metric
```

Scenarios/Problems	Solution

How do I know the replication mode for the system?	Use the **show platform software multicast ip capability** command. The command displays the replication mode. There are two replication mode: Ingress and Egress.
	
	In Ingress mode, the ingress DFC line card or the SP (in case the packets arrive on a non DFC line card) replicates for each of the outgoing interfaces. The ingress EARL does a lookup and sends the result to the replication engine to perform the replication of the packets.
	
	In Egress mode, the ingress line card just transmits one copy of the packet to each of the egress line card which is a DFC. The DFC looks for the packet and replicates the interfaces local to its line card. This mode of replication is better from the fabric backplane utilization perspective. The special unique EGRESS VLAN is used for sending the packet to the egress line card. This is the output of s**how vlan internal usage | i Egress multicast**.
	
	`7606-3#`
	`7606-3(config)#`**`ip multicast hardware-switching`** `replication-mode egress`
	`Warning: This command will change the replication mode for all address families.`
	`Warning: Egress replication-mode forced by CLI in presence of an egress-incapable card`
	`7606-3(config)#`
	`02:09:02: %CONST_MFIB_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected. Current system replication mode is Egress`
	`7606-3(config)#end`
	`7606-3#`
	`7606-3`**`#show platform software multicast ip capability`**
	
	`Current System HW Replication Mode : Egress`
	`Auto-detection of Replication Mode : OFF`
	
	`Slot Replication-Capability Replication-Mode`
	`1 Ingress Egress`
	`2 Egress Egress`
	`4 Egress Egress`
	`5 Egress Egress`
	`7606-3#`

Scenarios/Problems	Solution
	7606-3#**show vlan internal usage | i Egress multicast** 1015 IPv4 VPN 0 Egress multicast 7606-3# 7606-3#**conf t** Enter configuration commands, one per line. End with CNTL/Z. 7606-3(config)#**ip multicast hardware-switching** replication-mode ingress Warning: This command will change the replication mode for all address families. 7606-3(config)#end 7606-3# 02:11:54: %CONST_MFIB_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected. Current system replication mode is Ingress 7606-3# 7606-3#**show platform software multicast ip capability** Current System HW Replication Mode : Ingress Auto-detection of Replication Mode : OFF Slot Replication-Capability Replication-Mode 1 Ingress Ingress 2 Egress Ingress 4 Egress Ingress 5 Egress Ingress 7606-3#
How do I display information about the internal VLAN allocation?	Use the **show vlan internal usage** command in privileged EXEC mode. These are internal vlans which are used by the 7600 platform. The scope of these vlans are limited to the box and has no meaning outside the scope of the box. Each vlan corresponds to one interface on the Cisco 7600 router. This sample output is of the IIF and OIF being represented as a VLAN. 7606-3#s**how vlan internal usage | i 1028** 1028 FastEthernet1/13 **<<<<< Internal vlan 1028 is** mapped to interface Fa1/13 7606-3#

Scenarios/Problems	Solution

How do I identify the features enabled on the VLAN?	Use the **show mls vlan-ram** command. The command displays the features enabled on VLAN. It also helps you to validate the VLAN to MLS VPN mapping. MLS VPN is different from IOS VPN, and used for HW switching. This is a sample output from the command:
	`sp#show mls vlan-ram 1029 1031`
	`vlan eom nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro rpf-pbr-ovr`
	`----+---+------+----+-------+------+-----+---+-------+-------+---- ----+-----------`
	`1029 - - * 0 0 - - 0 0 - *`
	`1030 - - * 0 0 - - 260 0 - *`
	`1031 - - * 0 0 - - 261 0 - *`
	
	In the above output, the VLAN 1030 has MPLS VPN number 260 assigned to it. This may be different from IOS VPN number.

How do I know the MPLS label and COS bits used for the VPN number?	Use the **show mls vpn-cam** command. The command displays MPLS label and COS bits used for the VPN number. This is a sample output from the command:
	`ESM-20G-2#show mls vpn-cam start 0 end 0 all`
	`TYCHO Sindex VPN RAM: Dumping entries 0 -> 0`
	`Key: * => Set, - => Clear`
	
	`Index MPLS Label VPN COS`
	`=====+============+======+=====`
	`0 0 0 0`
	`ESM-20G-2#`