CHAPTER 32

Configuring IGMP Snooping and MVR for IPv4 Multicast Traffic

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping, including an application of local IGMP snooping, Multicast VLAN Registration (MVR) for IPv4 multicast traffic in Cisco IOS Software Release 12.2SX.

Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Software Releases 12.2SX Command References at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/122sx_mcl.html

- To constrain IPv6 Multicast traffic, see Chapter 30, "Configuring MLD Snooping for IPv6 Multicast Traffic."

This chapter consists of these sections:

Understanding IGMP Snooping

These sections describe IGMP snooping:

IGMP Snooping Overview

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.

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 31, "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 "Enabling the IGMP Snooping Querier" section on page 32-9.

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 32-1).

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 32-1 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 32-1, that includes the port numbers of Host 1, the multicast router, and the switch internal CPU.

Table 32-1 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 32-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 32-2. 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 32-2 Second Host Joining a Multicast Group

Table 32-2 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 32-4
- Fast-Leave Processing, page 32-5

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." 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 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.

Understanding IGMP Version 3 Support

These sections describe IGMP version 3 support:

- IGMP Version 3 Support Overview, page 32-6
- IGMPv3 Fast-Leave Processing, page 32-6

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 32-3 shows the default IGMP snooping configuration.

Table 32-3 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 32-3 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/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfmulti.htm
- 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:

- The IGMP snooping querier does not support querier elections. Enable the IGMP snooping querier on only one switch in the VLAN. (CSCsk48795)
- Configure the VLAN in global configuration mode (see Chapter 17, "Configuring VLANs").
- Configure an IP address on the VLAN interface (see Chapter 24, "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 after 60 seconds with no IGMP traffic detected from a multicast router. 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.

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`	Enables the IGMP snooping querier.
	`Router(config-if)# no ip 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 31, "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 32-9).

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

These sections describe how to configure IGMP snooping:

- CGMP Automatic Detection, page 32-13
- Displaying IGMP Snooping Information, page 32-14

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.
	`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* = **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* = **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
```

Configuring the IGMP Snooping 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 interval for the IGMP snooping queries sent by the switch, 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 switch. 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

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.
	`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 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/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtssmma.htm

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 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

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 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#
```

Understanding MVR

Release 12.2(33)SXH and later releases support Multicast VLAN Registration (MVR). MVR is designed for applications that use wide-scale deployment of multicast traffic across an Ethernet ring-based service-provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP Version-2-compatible host with an Ethernet connection. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One feature can be enabled or disabled without affecting the operation of the other feature. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

MVR does the following:

- Identifies the MVR IP multicast streams and their associated IP multicast group in the Layer 2 forwarding table.
- Intercepts the IGMP messages.
- Modifies the Layer 2 forwarding table to include or remove the subscriber as a receiver of the multicast stream, even though the receivers might be in a different VLAN from the source.

This forwarding behavior selectively allows traffic to cross between different VLANs.

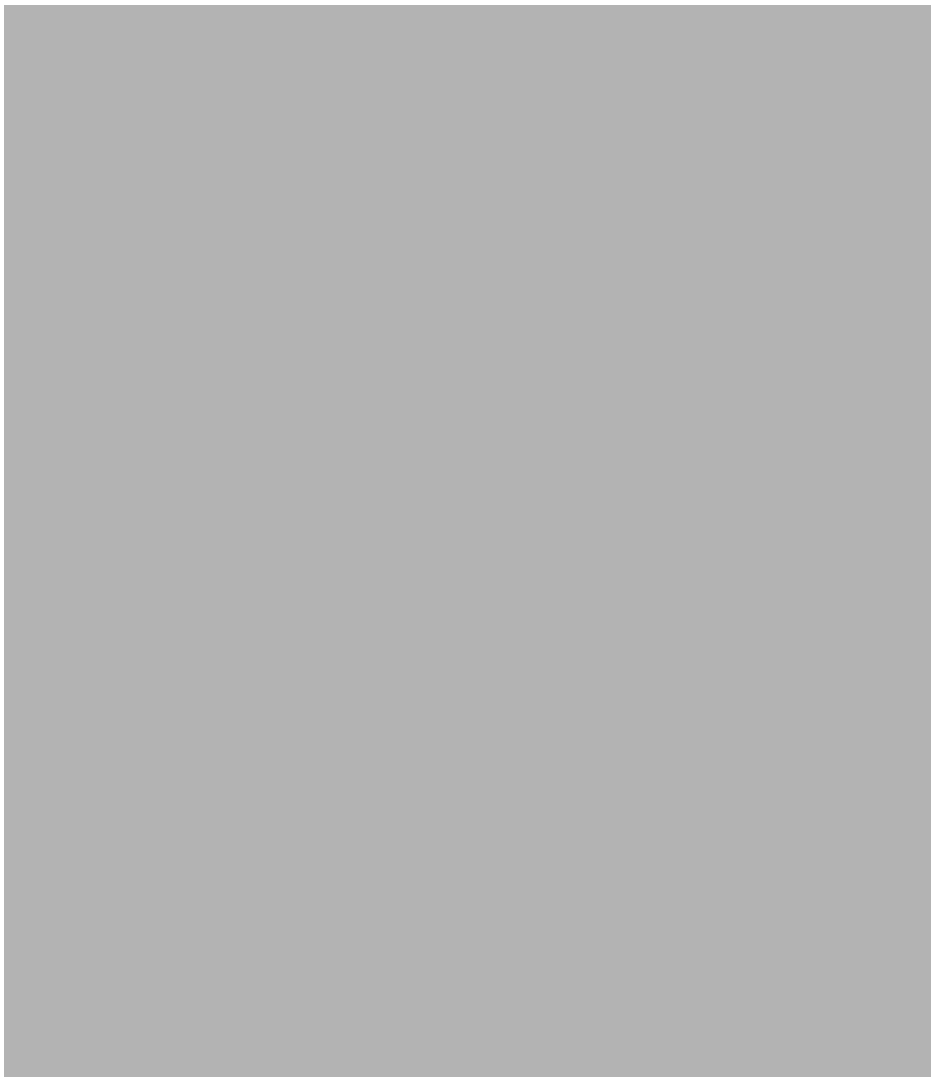
The switch will forward multicast data for MVR IP multicast streams only to MVR ports on which hosts have joined, either by IGMP reports or by MVR static configuration. The switch will forward IGMP reports received from MVR hosts only to the source (uplink) port. This eliminates using unnecessary bandwidth on MVR data port links.

Only Layer 2 ports participate in MVR. You must configure ports as MVR receiver ports. Only one MVR multicast VLAN per switch.

Using MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. Figure 32-3 is an example configuration. DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to Switch A to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the SP CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

Figure 32-3 Multicast VLAN Registration Example



When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The SP CPU sends a MAC-based general query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

Unless the Immediate Leave feature is enabled, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With the Immediate Leave feature enabled, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency. Enable the Immediate Leave feature only on receiver ports to which a single receiver device is connected.

MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is only sent around the VLAN trunk once—only on the multicast VLAN. The IGMP leave and join messages are in the VLAN to which the subscriber port is assigned.

These messages dynamically register for streams of multicast traffic in the multicast VLAN on the Layer 3 device, Switch B. The access layer switch, Switch A, modifies the forwarding behavior to allow the traffic to be forwarded from the multicast VLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

IGMP reports are sent to the same IP multicast group address as the multicast data. The Switch A CPU must capture all IGMP join and leave messages from receiver ports and forward them to the multicast VLAN of the source (uplink) port.

Configuring MVR

These sections contain this configuration information:

Default MVR Configuration

Table 32-4 shows the default MVR configuration.

Table 32-4 Default MVR Configuration

Feature	Default Setting
MVR	Disabled globally and per interface
Multicast addresses	None configured
Query response time	1 second
Multicast VLAN	VLAN 1
Interface (per port) default	Neither a receiver nor a source port
Immediate Leave	Disabled on all ports

MVR Configuration Guidelines and Limitations

When configuring MVR, follow these guidelines:

- Only one MVR VLAN can be present in a switch, and you should configure the same VLAN as the MVR VLAN for all the switches in the same network.
- Source ports must be in the MVR VLAN.
- Receiver ports on a switch can be in different VLANs, but must not be in the MVR VLAN.
- Receiver ports can only be access ports; they cannot be trunk ports.
- When using private VLANs, you cannot configure a secondary VLAN as the MVR VLAN.
- Do not connect a multicast router to a receiver port.
- The MVR VLAN must not be a reverse path forwarding (RPF) interface for any multicast route.
- MVR data received on an MVR receiver port is not forwarded to MVR source ports.
- The maximum number of multicast entries (MVR group addresses) that can be configured on a switch (that is, the maximum number of television channels that can be received) is 8000.
- MVR on IPv6 multicast groups is not supported.
- MVR is available only on native systems.
- VTP pruning should be disabled if the MVR VLAN number is between 1 and 1000.
- MVR can coexist with IGMP snooping on a switch.
- MVR supports IGMPv3 messages.

Configuring MVR Global Parameters

You do not need to set the optional MVR parameters if you choose to use the default settings. Before changing the default parameters (except for the MVR VLAN), you must first enable MVR.

Note For complete syntax and usage information for the commands used in this section, see the Cisco IOS Software Releases 12.2SX Command References.

To configure the MVR global parameters, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# mvr`	Enables MVR on the switch.
Step 3	`Router(config)# mvr max-groups` *max-groups*	Specifies the maximum number of MVR groups. The range is 1 to 8000. The default is 1000.

	Command	Purpose
Step 4	`Router(config)# mvr group ip-address [count]`	Configures an IP multicast address on the switch or uses the *count* parameter to configure a contiguous series of MVR group addresses (the range for *count* is 1 to 256; the default is 1). Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address. Each multicast address would correspond to one television channel.
Step 5	`Router(config)# mvr querytime value`	(Optional) Defines the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 1 to 100, and the default is 10 tenths or one second.
Step 6	`Router(config)# mvr vlan vlan-id`	(Optional) Specifies the VLAN in which multicast data is received; all source ports must belong to this VLAN. The VLAN range is 1 to 1001 and 1006 to 4094. The default is VLAN 1.
Step 7	`Router(config)# end`	Returns to privileged EXEC mode.
Step 8	`Router# show mvr`	Verifies the configuration.

To return the switch to its default settings, use the **no mvr** [**group** *ip-address* | **querytime** | **vlan**] global configuration command.

This example shows how to enable MVR, configure the group address, set the query time to 1 second (10 tenths), and specify the MVR multicast VLAN as VLAN 22:

```
Router(config)# mvr
Router(config)# mvr group 228.1.23.4
Router(config)# mvr querytime 10
Router(config)# mvr vlan 22
Router(config)# end
```

You can use the **show mvr groups** privileged EXEC command to verify the MVR multicast group addresses on the switch.

Configuring MVR Interfaces

To configure Layer 2 MVR interfaces, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# mvr`	Enables MVR on the switch.
Step 3	`Router(config)# interface interface-id`	Specifies the Layer 2 port to configure, and enters interface configuration mode.

	Command	Purpose
Step 4	`Router(config-if)# mvr type {source | receiver}`	Configures an MVR port as one of these types of ports: • **source**—Configures uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN. • **receiver**—Configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails. The default configuration is as a non-MVR port.
Step 5	`Router(config-if)# mvr immediate`	(Optional) Enables the Immediate Leave feature of MVR on the port. The Immediate Leave feature is disabled by default. **Note** This command applies to only receiver ports and should only be enabled on receiver ports to which a single receiver device is connected.
Step 6	`Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	`Router# show mvr`	Verifies the configuration.

To return the interface to its default settings, use the **no mvr** [**type** | **immediate**] interface configuration commands.

This example shows how to configure a source port and a receiver port and to configure Immediate Leave on the receiver port:

```
Router(config)# mvr
Router(config)# interface gigabitethernet 3/48
Router(config-if)# switchport
Router(config-if)# switchport access vlan 22
Router(config-if)# mvr type source
Router(config-if)# exit
Router(config)# interface gigabitethernet 3/47
Router(config-if)# switchport
Router(config-if)# switchport access vlan 30
Router(config-if)# mvr type receiver
Router(config-if)# mvr immediate
Router(config-if)# exit
Router(config)#
```

Displaying MVR Information

You can display MVR information for the switch or for a specified interface. To display MVR configurations, perform one or more of these tasks:

Command	Purpose
`Router# show mvr`	Displays MVR status and these values for the switch: whether MVR is enabled or disabled, the multicast VLAN, the configured maximum and current number of multicast groups, and the query response time.
`Router# show mvr groups`	Displays the MVR group configuration.
`Router# show mvr interface` [*type module/port*]	Displays all MVR interfaces and their MVR configurations. When a specific interface is entered, displays this information: • Type—Receiver or Source • Status—One of these: – Active—At least one IGMP join has been received for an MVR group on the port. – Inactive—The port is not participating in any MVR groups. – Up/Down—The port is forwarding (Up) or nonforwarding (Down). • Immediate Leave—Enabled or Disabled
`Router# show mvr members` [[**vlan** *vlan-id*] | [*type module/port*]]	Displays details of all MVR members or MVR members on a specified VLAN or port.
`Router# show mvr members` [[**vlan** *vlan-id*] | [*type module/port*]] **count**	Displays number of MVR members in all active MVR groups. or on a specified VLAN or port.
`Router# show mvr` {**receiver-ports** | **source-ports**} [*type module/port*]	Displays all receiver or source ports that are members of any IP multicast group or those on the specified interface port.

This example displays MVR status and values for the switch:

```
Router# show mvr
MVR Running: TRUE
MVR multicast vlan: 22
MVR Max Multicast Groups: 1000
MVR Current multicast groups: 256
MVR Global query response time: 10 (tenths of sec)
```

This example displays the MVR group configuration:

```
Router# show mvr groups
MVR max Multicast Groups allowed: 8000
MVR current multicast groups: 8000
MVR groups:
        Group start     Group end       Type  Count/Mask
        --------------- --------------- ----- ---------------
        225.0.7.226     225.0.7.226     count 1
        225.0.7.227     225.0.7.227     count 1
        225.0.7.228     225.0.7.228     count 1
```

```
        225.0.7.229     225.0.7.229     count 1
        225.0.7.230     225.0.7.230     count 1
        225.0.7.231     225.0.7.231     count 1
        236.8.7.0       236.8.7.255     mask  255.255.255.0
        237.8.7.0       237.8.7.255     mask  255.255.255.0
        237.8.8.0       237.8.8.255     mask  255.255.255.0
```

This example displays all MVR interfaces and their MVR configurations:

```
Router# show mvr interface
Port      VLAN  Type       Status           Immediate Leave
----      ----  ----       ------           ---------------
Gi1/20       2  RECEIVER   ACTIVE/UP        DISABLED
Gi1/21       2  SOURCE     ACTIVE/UP        DISABLED
```

This example displays all MVR members on VLAN 2:

```
Router# show mvr members vlan 2
MVR Group IP     Status    Members
------------     ------    -------
224.000.001.001   ACTIVE    Gi1/20(u),Gi1/21(u)
224.000.001.002   ACTIVE    Fa3/2(d),Gi1/12(u)
```

This example displays the number of MVR members on all MVR VLANs:

```
Router# show mvr members count

Count of active MVR groups:
    Vlan 490: 400
    Vlan 600: 400
    Vlan 700: 0
    Vlan 950: 0
```

This example displays all receiver ports that are members of any IP multicast group:

```
Router# show mvr receiver-ports
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port   VLAN Status         Immediate          Joins
                          Leave        (v1,v2,v3)     (v3)
----   ---- -------------  -----------   ---------- -----------
Gi1/7   202 INACTIVE/UP    ENABLED          305336           0
Gi1/8   202 ACTIVE/UP     DISABLED           4005           0
Gi1/9   203 INACTIVE/DOWN  DISABLED          53007           0
Gi1/10  203 ACTIVE/UP     DISABLED           6204           0
Gi1/11  204 ACTIVE/UP     DISABLED             0          940
Gi1/12  205 INACTIVE/UP    ENABLED            8623           0
```

Clearing MVR Counters

You can clear MVR join counters for the switch, for source or receiver ports, or for a specified interface.

To clear MVR counters, perform this task:

Command	Purpose
Router# **clear mvr counters** [[**receiver-ports** | **source-ports**] [*type module/port*]]	Clears the join counters of all the MVR ports, or source or receiver ports, or of a specified MVR interface port.

This example clears the join counters for the receiver port on GigabitEthernet port 1/7:

```
Router# clear mvr receiver-ports GigabitEthernet 1/7
Router# show mvr receiver-ports GigabitEthernet 1/7
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port   VLAN Status         Immediate          Joins
                           Leave        (v1,v2,v3)     (v3)
----   ---- -------------  ----------   ---------- -----------
Gi1/7   202 INACTIVE/UP    ENABLED              0           0
```