Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

Note

- 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 12.1, "IP Multicast," "Configuring IP Multicast Routing," at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/1cdmulti.htm
- For more information on IP multicast and IGMP, refer to RFC 1112 and RFC 2236.

Understanding How IGMP Snooping Works

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 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward 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 18, "Configuring IP Multicast Layer 3 Switching."

With Release 12.1(8a)E and later releases, you can configure the IGMP snooping querier on the switch to support IGMP snooping in subnets that do not have any multicast router interfaces because the multicast traffic does not need to be routed. For more information about the IGMP snooping querier, see the "Enabling the IGMP Snooping Querier" section on page 21-7.

IGMP (on a multicast router) or the IGMP snooping querier (on the supervisor engine) 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).

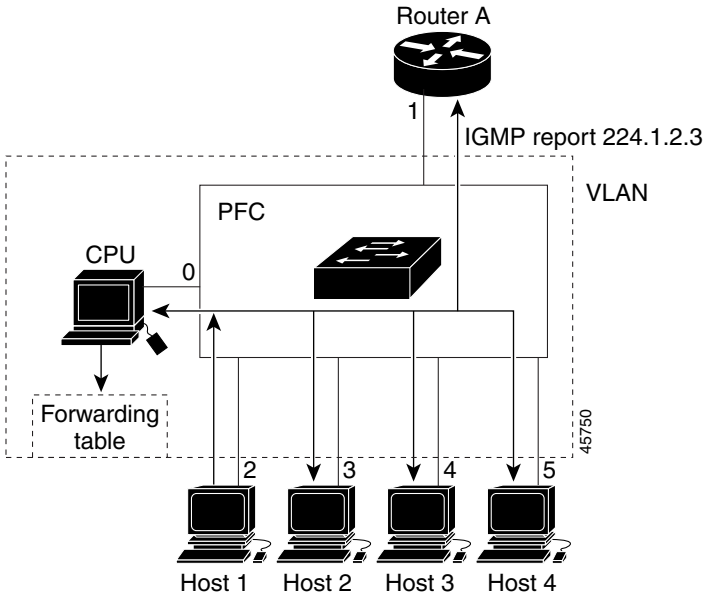
In response to an IGMP join request, the switch creates an entry in its Layer 2 forwarding table for the VLAN on which the join request was received. When other hosts interested in this multicast traffic send IGMP join requests, the switch adds them to the existing Layer 2 forwarding table entry. The 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 21-1.

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 21-1 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 21-1, that includes the port numbers of Host 1, the multicast router, and the switch internal CPU.

Table 21-1 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 21-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 21-2. 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 21-2 Second Host Joining a Multicast Group

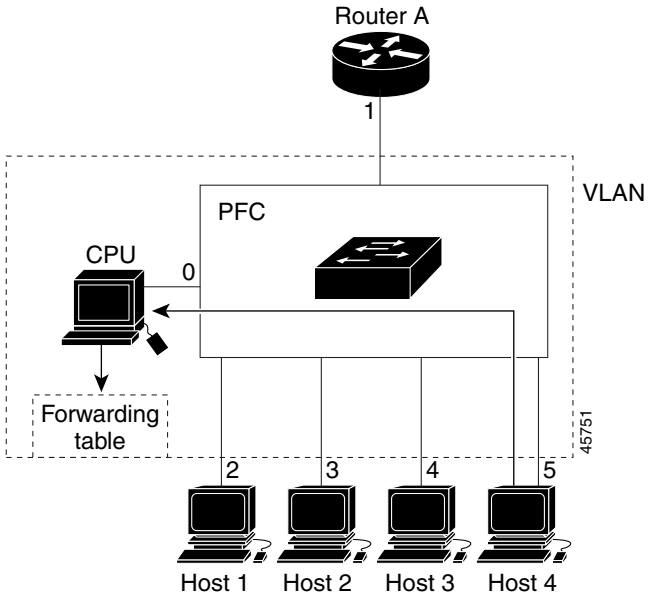


Table 21-2 Updated IGMP Snooping Forwarding Table

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 21-4
- Fast-Leave Processing, page 21-5

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 a group-specific 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." Enter the **ip igmp snooping last-member-query-interval** *interval* command to configure the interval.

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 IGMP Snooping Querier

IGMP snooping querier should be used 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 with IP multicast routing, the IP multicast router acts as the IGMP querier. If the IP-multicast traffic in a VLAN needs to be Layer 2 switched only, an IP-multicast router is not required, but without an IP-multicast router on a VLAN, you must configure another switch as the IGMP querier so that it can send queries.

When IGMP snooping querier is enabled, the IGMP snooping querier sends out periodic IGMP 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.

You can enable the IGMP snooping querier on all the Catalyst 6500 series switches in the VLAN, but for each VLAN that is connected to switches that use IGMP to report interest in IP multicast traffic, you must set at least one switch as the IGMP snooping querier.

You can use Cisco IOS commands to configure the Catalyst 6500 series switches to generate such IGMP queries on a VLAN regardless of whether or not IP multicast routing is enabled.

Note To enable IP multicast routing on the Catalyst 6500 series switches on a specific VLAN, enter the **ip pim sparse-mode** command, the **ip pim sparse-dense-mode** command, or the **ip pim dense-mode** command on that interface. See Chapter 18, "Configuring IP Multicast Layer 3 Switching" for more details.

Understanding IGMP Version 3 Support

With Release 12.1(8a)E and later releases, IGMP snooping supports IGMP version 3. 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. A single multicast source per group allows IGMPv3 hosts connected to specific ports to receive traffic from a specific (source, group).

Default IGMP Snooping Configuration

Table 21-3 shows the default IGMP snooping configuration.

Table 21-3 IGMP Snooping Default Configuration

Feature	Default Values
IGMP snooping querier[1]	Disabled
IGMP snooping	Enabled
Multicast routers	None configured
IGMP snooping learning method	PIM/DVMRP[2]

1. Supported in Release 12.1(8a)E and later releases.
2. PIM/DVMRP = Protocol Independent Multicast/Distance Vector Multicast Routing Protocol

IGMP Snooping and IGMP Snooping Querier Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring IGMP snooping and IGMP snooping querier:

Guidelines

- 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.
- 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.
- You can enable the IGMP snooping querier on all the Catalyst 6500 series switches in the VLAN. On each VLAN that is connected to switches that use IGMP to report interest in IP multicast traffic, you must set one switch as the IGMP querier.

Periodically, the IGMP querier sends IGMP 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. In a normal network with IP multicast routing, the IP multicast router acts as the IGMP querier.

Note To enable IP multicast routing on the Catalyst 6500 series switches on a specific VLAN, enter the **ip pim sparse-mode** command, the **ip pim sparse-dense-mode** command, or the **ip pim dense-mode** command on that interface. See Chapter 18, "Configuring IP Multicast Layer 3 Switching" for more details.

- If the IP-multicast traffic in a VLAN needs to be Layer 2 switched only, an IP-multicast router is not required, but without an IP-multicast router on a VLAN, you must configure another switch as the IGMP querier so that it can send queries. You can use Cisco IOS commands to configure the Catalyst 6500 series switches to generate such IGMP queries on a VLAN regardless of whether or not IP multicast routing is enabled.

Restrictions

- IGMP snooping querier requires Release 12.1(8a)E and later.
- When configuring the IGMP snooping querier, configure the VLAN in the VLAN database or, with Release 12.1(11b)E and later releases, configure the VLAN in global configuration mode (see Chapter 9, "Configuring VLANs").
- QoS does not support IGMP packets when IGMP snooping is enabled.
- You must configure an IP address on the VLAN interface for the IGMP snooping querier to start. (See Chapter 12, "Configuring Layer 3 Interfaces"). When enabled, the IGMP snooping querier uses the IP address as the query source address. The IGMP snooping querier disables itself if the IP address is cleared and restarts when you configure an IP address.

Note With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Enabling the IGMP Snooping Querier

With Release 12.1(8a)E and later, 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 igmp snooping querier`	Enables the IGMP snooping querier.
	`Router(config-if)# no ip igmp snooping querier`	Disables the IGMP snooping querier.

	Command	Purpose
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`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)# 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 18, "Configuring IP Multicast Layer 3 Switching") or enable the IGMP snooping querier in the subnet (see the "Enabling the IGMP Snooping Querier" section on page 21-7).

IGMP snooping allows Catalyst 6500 series switches to examine IGMP packets and make forwarding decisions based on their content.

These sections describe how to configure IGMP snooping:

- Enabling IGMP Snooping, page 21-9
- Configuring IGMP Snooping Learning, page 21-10
- Configuring a Multicast Router Port Statically, page 21-10
- Configuring the IGMP Query Interval, page 21-11
- Enabling IGMP Fast-Leave Processing, page 21-11
- Configuring a Host Statically, page 21-12
- Displaying IGMP Snooping Information, page 21-12

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 200 and verify the configuration:

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

Configuring IGMP Snooping Learning

To configure IGMP snooping learning, 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 mrouter learn {cgmp | pim-dvmrp}`	Configures the learning method.
	`Router(config-if)# no ip igmp snooping mrouter learn {cgmp | pim-dvmrp}`	Reverts to the default learning method.

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

```
Router(config)# interface vlan 1
Router(config-if)# ip igmp snooping mrouter learn pim-dvmrp
Router(config-if)# end
Router#
```

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

```
Router(config)# interface vlan 1
Router(config-if)# ip igmp snooping mrouter learn cgmp
Router(config-if)# end
Router#
```

Configuring a Multicast Router Port Statically

To configure a static connection to a multicast router, 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 router.
	`Router(config)# no mac-address-table static mac_addr vlan vlan_id`	Clears a static connection to a multicast router.
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**

With Release 12.1(11b)E2 and later releases, you can enter the **disable-snooping** keyword to prevent multicast traffic addressed to the statically configured multicast MAC address from also being sent to other multicast router ports in the same VLAN.

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

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

All releases support the **mac-address-table static** command. The **ip igmp snooping mrouter interface** command, which was available in earlier releases and which provided the same functionality as the **mac-address-table static** command, is deprecated in Release 12.1(13)E and later releases.

Configuring the IGMP 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 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 queries sent by the switch. Default is 1 second. Valid range is 100 to 999 milliseconds.
	`Router(config-if)# no ip igmp snooping last-member-query-interval`	Reverts to the default value.

This example shows how to configure the IGMP 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-member-query-interval
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 a Host Statically

Hosts normally join multicast groups dynamically, but you can also configure a host statically for a Layer 2 LAN port.

To configure a host statically for a Layer 2 LAN port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects a VLAN interface.
Step 2	`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 router.
	`Router(config)# no mac-address-table static mac_addr vlan vlan_id`	Clears a static connection to a multicast router.

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

With Release 12.1(11b)E2 and later releases, you can enter the **disable-snooping** keyword to prevent multicast traffic addressed to the statically configured multicast MAC address from being sent to multicast router ports in the same VLAN.

This example shows how to configure a host statically in VLAN 12 on FastEthernet port 5/7:

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

All releases support the **mac-address-table static** command. The **ip igmp snooping static** command, which was available in earlier releases and which provided the same functionality as the **mac-address-table static** command, is deprecated in Release 12.1(13)E and later releases.

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 multicast routers are connected.

To display multicast router interfaces, perform this task:

Command	Purpose
`Router# show ip igmp snooping mrouter interface 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 interface 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 200
Vlan200 is up, line protocol is up
  Internet address is 172.20.52.94/27
  IGMP is enabled on interface
  Current IGMP version is 2
  CGMP is disabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 0 joins, 0 leaves
  Multicast routing is enabled on interface
```

```
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 172.20.52.94 (this system)
  IGMP querying router is 172.20.52.94 (this system)
  No multicast groups joined
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave is enabled on this interface
  IGMP snooping querier is disabled on this interface
Router#
```