



# Understanding and Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 4006 switch with Supervisor Engine III. It also provides guidelines, procedures, and configuration examples.

This chapter consists of the following sections:

- [IGMP Snooping Overview, page 17-1](#)
- [Default IGMP Snooping Configuration, page 17-3](#)
- [IGMP Snooping Configuration Guidelines and Restrictions, page 17-3](#)
- [Configuring IGMP Snooping, page 17-3](#)



**Note**

To support Cisco Group Management Protocol (CGMP) client devices, configure the switch as a CGMP server. For more information, refer to the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1, “IP Multicast,” “Configuring IP Multicast Routing,” at the following URL: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt3/1cdmulti.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/1cdmulti.htm)



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference for the Catalyst 4006 Switch with Supervisor Engine III* and the publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## IGMP Snooping Overview

In subnets where you have configured IGMP, IGMP snooping manages multicast traffic at Layer 2 by configuring interfaces that have been set up using the **switchport** keyword to dynamically forward multicast traffic only to those interfaces that want to receive it.

IGMP snooping constrains traffic in MAC multicast groups 01-00-5e-00-00-01 to 01-00-5e-ff-ff-ff. IGMP snooping does not constrain Layer 2 multicast packets generated by routing protocols.



**Note**

For more information on IP multicast and IGMP, refer to RFC 1112 and RFC 2236.

IGMP (on a router) sends out periodic general IGMP queries. When you enable IGMP snooping, the switch responds at Layer 2 to the IGMP queries with only one IGMP join request per Layer 2 multicast group. The switch creates one entry per subnet in the Layer 2 forwarding table for each Layer 2 multicast group from which it receives an IGMP join request. All hosts interested in this multicast traffic send IGMP join requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **ip igmp snooping static** command. If you specify group membership for a multicast group address statically, your static setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

Groups with IP addresses in the 224.0.0.\* range are reserved for routing control packets and are flooded to all forwarding ports of the VLAN. These addresses map to the multicast MAC address range 01-00-5E-00-00-xx, where xx is in the range 0-0xFF.

**Note**

If a spanning-tree topology change occurs in a VLAN, then IP multicast traffic floods in all ports in the VLAN where PortFast is not enabled for three general query intervals.

When a host connected to a Layer 2 interface wants to join an IP multicast group, it sends an IGMP join request specifying the IP multicast group it wants to join. When hosts want to leave a multicast group, they can either ignore the periodic general IGMP queries, or they can send an IGMP leave message. When the switch receives an IGMP leave message from a host, it sends out a group-specific IGMP query to determine if any devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the table entry for that Layer 2 multicast group so that only those hosts interested in receiving multicast traffic for the group are listed.

## Fast-Leave Processing

IGMP snooping fast-leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

When a switch with IGMP snooping enabled receives an IP group-specific IGMPv2 leave message, it sends a group-specific query out the interface where the leave message was received to determine if there are any other hosts attached to that interface that are interested in the MAC multicast group. If the switch does not receive an IGMP join message within the query-response-interval and none of the other 31 IP groups corresponding to the MAC group are interested in the multicast traffic for that MAC group and no multicast routers have been learned on the interface, then the interface is removed from the port list of the (mac-group, vlan) entry in the L2 forwarding table. With fast-leave enabled on the VLAN, an interface can be removed immediately from the port list of the L2 entry when the IGMP leave message is received, unless a multicast router was learned on the port.

**Note**

Use fast-leave processing only on VLANs where only one host is connected to each interface. If fast-leave is enabled in VLANs where more than one host is connected to an interface, some hosts might be dropped inadvertently. Immediate-leave processing is supported only with IGMP version 2 hosts.

# IGMP Snooping Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring the IGMP:

- Configure the VLAN in the VLAN database (see [Chapter 7, “Understanding and Configuring VLANs”](#)).
- QoS does not apply IGMP packets when IGMP snooping is enabled.

## Default IGMP Snooping Configuration

[Table 17-1](#) shows the default IGMP snooping configuration.

**Table 17-1 IGMP Snooping Default Configuration**

Feature	Default Values
IGMP snooping	Enabled
Multicast routers	None configured
IGMP snooping learning method	PIM/DVMRP <sup>1</sup>

1. PIM/DVMRP = Protocol Independent Multicast/Distance Vector Multicast Routing Protocol

## Configuring IGMP Snooping



### Note

To use IGMP snooping, configure a Layer 3 interface in the subnet for multicast routing (see [Chapter 15, “Understanding and Configuring IP Multicast”](#)).

IGMP snooping allows 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 17-4](#)
- [Configuring Learning, page 17-4](#)
- [Configuring a Multicast Router Port Statically, page 17-5](#)
- [Enabling IGMP Fast-Leave Processing, page 17-6](#)
- [Configuring a Host Statically, page 17-6](#)
- [Displaying IGMP Snooping Information, page 17-7](#)

## Enabling IGMP Snooping

To enable IGMP snooping globally, perform this task:

	Task	Command
<b>Step 1</b>	Enable IGMP snooping.	Switch(config)# <b>[no] ip igmp snooping</b>
	Use the <b>no</b> keyword to disable IGMP snooping.	
<b>Step 2</b>	Exit configuration mode.	Switch(config)# <b>end</b>
<b>Step 3</b>	Verify the configuration.	Switch# <b>show ip igmp snooping   include globally</b>

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

```
Switch(config)# ip igmp snooping
Switch(config)# end
Switch# show ip igmp snooping | include globally
IGMP snooping is globally enabled
Switch#
```

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

	Task	Command
<b>Step 1</b>	Enable IGMP snooping.	Switch(config)# <b>[no] ip igmp snooping vlan vlan_ID</b>
	Use the <b>no</b> keyword to disable IGMP snooping.	
<b>Step 2</b>	Exit configuration mode.	Switch(config)# <b>end</b>
<b>Step 3</b>	Verify the configuration.	Switch# <b>show ip igmp snooping vlan vlan_ID</b>

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200
Switch(config)# end
Switch# show ip igmp snooping vlan 200
vlan 200
IGMP snooping is globally enabled
IGMP snooping is enabled on this VLAN
IGMP snooping intermediate-leave is disabled on this VLAN
IGMP snooping mrouter learn mode is pim-dvmrp on this VLAN
IGMP snooping is running in IGMP_ONLY mode on thei VLAN
Switch#
```

## Configuring Learning

The following sections describe IGMP snooping learning methods:

- [Configuring IGMP Learning, page 17-5](#)
- [Configuring CGMP Learning, page 17-5](#)

## Configuring IGMP Learning

To configure IGMP snooping to learn from PIM/DVMRP packets, enter the following command:

Command	Purpose
Switch(config)# <b>ip igmp snooping vlan</b> <i>vlan_ID</i> <b>mrouter learn</b> [ <b>cgmp</b>   <b>pim-dvmrp</b> ]	Specifies the learning method for the VLAN.

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

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

## Configuring CGMP Learning

To configure IGMP snooping to learn from CGMP self-join packets, enter the following command:

Command	Purpose
Switch(config)# <b>ip igmp snooping vlan</b> <i>vlan_ID</i> <b>mrouter learn</b> [ <b>cgmp</b>   <b>pim-dvmrp</b> ]	Specifies the learning method for the VLAN.

This example shows how to configure IP IGMP snooping to use CGMP self-join packets as the learning method:

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
Switch#
```

## Configuring a Multicast Router Port Statically

To configure a static connection to a multicast router, enter the **ip igmp snooping mrouter** command on the switch instead of the **ip cgmp router-only** command.

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

Task	Command
<b>Step 1</b> Specify the a static connection to a multicast router for the VLAN.  <b>Note</b> The interface to the router must be in the VLAN where you are entering the command and it must be administratively up and the line protocol must be up.	Switch(config)# <b>ip igmp snooping vlan</b> <i>vlan_ID</i> <b>mrouter interface</b> <i>interface_num</i>
<b>Step 2</b> Exit configuration mode.	Switch(config)# <b>end</b>
<b>Step 3</b> Verify the configuration.	Switch# <b>show ip igmp snooping mrouter vlan</b> <i>vlan_ID</i>

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

```
Switch(config)# ip igmp snooping vlan 200 mrouter interface fastethernet 5/10
Switch# show ip igmp snooping mrouter vlan 200
vlan                ports
-----+-----
 200 Fa5/10
Switch#
```

## Enabling IGMP Fast-Leave Processing

When you enable IGMP fast-leave processing in a VLAN, the switch immediately removes an interface from the multicast group when it detects an IGMP version 2 leave message on that interface.

To enable IGMP fast-leave processing on an interface, enter the following command:

Command	Purpose
Switch(config)# <b>ip igmp snooping vlan <i>vlan_ID</i> immediate-leave</b>	Enables IGMP fast-leave processing in the VLAN.

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

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

## Configuring a Host Statically

Hosts normally join multicast groups dynamically, but you can also configure a host statically on an interface.

To configure a host statically on an interface, enter the following command:

Command	Purpose
Switch(config-if)# <b>ip igmp snooping vlan <i>vlan_ID</i> static <i>mac_address</i> interface <i>interface_num</i></b>	Configures a host statically in the VLAN.

This example shows how to configure a host statically in VLAN 200 on interface FastEthernet 5/11:

```
Switch(config)# ip igmp snooping vlan 200 static 0100.5e02.0203 interface fastethernet 5/11
Configuring port FastEthernet5/11 on group 0100.5e02.0203 vlan 200
Switch(config)#
```

## Displaying IGMP Snooping Information

The following sections describe displaying IGMP snooping information:

- [Displaying Multicast Router Interfaces, page 17-7](#)
- [Displaying MAC Address Multicast Entries, page 17-7](#)
- [Displaying IGMP Snooping Information for a VLAN Interface, page 17-8](#)

### 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, enter the following command:

Command	Purpose
Switch# <b>show ip igmp snooping mrouter vlan</b> <i>vlan_ID</i>	Displays multicast router interfaces.

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

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

### Displaying MAC Address Multicast Entries

To display MAC address multicast entries for a VLAN, enter the following command:

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

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

```
Switch# show mac-address-table multicast vlan 1
Multicast Entries
vlan  mac address      type      ports
-----+-----
 1    0100.5e01.0101     igmp     Switch,Gi6/1
 1    0100.5e01.0102     igmp     Switch,Gi6/1
 1    0100.5e01.0103     igmp     Switch,Gi6/1
 1    0100.5e01.0104     igmp     Switch,Gi6/1
 1    0100.5e01.0105     igmp     Switch,Gi6/1
 1    0100.5e01.0106     igmp     Switch,Gi6/1
Switch#
```

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

```
Switch# show mac-address-table multicast vlan 1 count
Multicast MAC Entries for vlan 1:    4
Switch#
```

## Displaying IGMP Snooping Information for a VLAN Interface

To display IGMP snooping information for a VLAN interface, enter the following command:

Command	Purpose
Switch# <b>show ip igmp interface vlan</b> <i>vlan_ID</i>	Displays IGMP snooping information on a VLAN interface.

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

```
Switch# show ip igmp interface vlan 200
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP-ONLY mode on this VLAN
Switch#
```