CHAPTER 25

Configuring IGMP Snooping and MVR

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the IE 3000 switch, including an application of local IGMP snooping, Multicast VLAN Registration (MVR). It also includes procedures for controlling multicast group membership by using IGMP filtering and procedures for configuring the IGMP throttling action.

Note For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the "IP Multicast Routing Commands" section in the *Cisco IOS IP Command Reference, Volume 3 of 3:Multicast, Release 12.2*
Documentation > Cisco IOS Software 12.2 Mainline Command References

This chapter consists of these sections:

- Understanding IGMP Snooping, page 25-1

Configuring IGMP Snooping, page 25-6

Displaying IGMP Snooping Information, page 25-15

Understanding Multicast VLAN Registration, page 25-16

Configuring MVR, page 25-19

Displaying MVR Information, page 25-22

Configuring IGMP Filtering and Throttling, page 25-23

Displaying IGMP Filtering and Throttling Configuration, page 25-28

You can either manage IP multicast group addresses through features such as IGMP snooping and MVR, or you can use static IP addresses.

Understanding IGMP Snooping

with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Note For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the **ip igmp snooping vlan** *vlan-id* *ip_address* *interface-id*

Configuring the IGMP Snooping Querier" section on page 25-13.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

- IGMP Versions, page 25-2
- Joining a Multicast Group, page 25-3
- Leaving a Multicast Group, page 25-5
- Immediate Leave, page 25-5
- IGMP Configurable-Leave Timer, page 25-5
- IGMP Report Suppression, page 25-6

IGMP Versions

Note

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008048a.html

Joining a Multicast Group

Figure 25-1 Initial IGMP Join Message

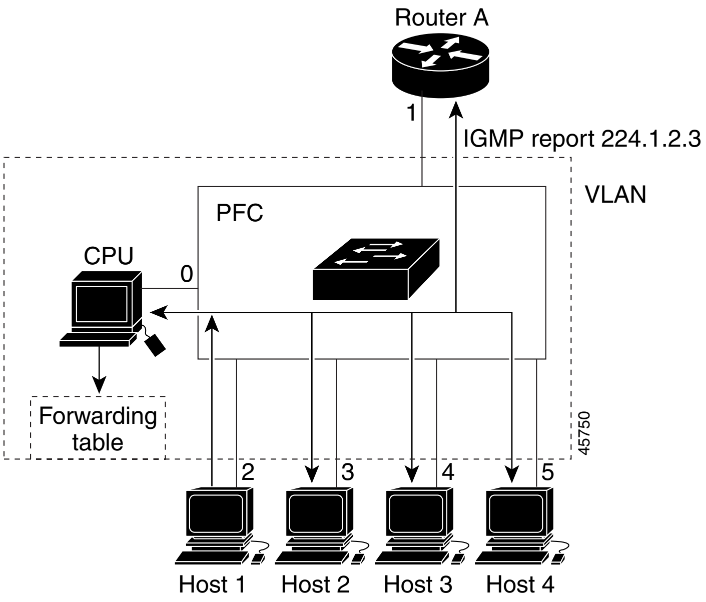
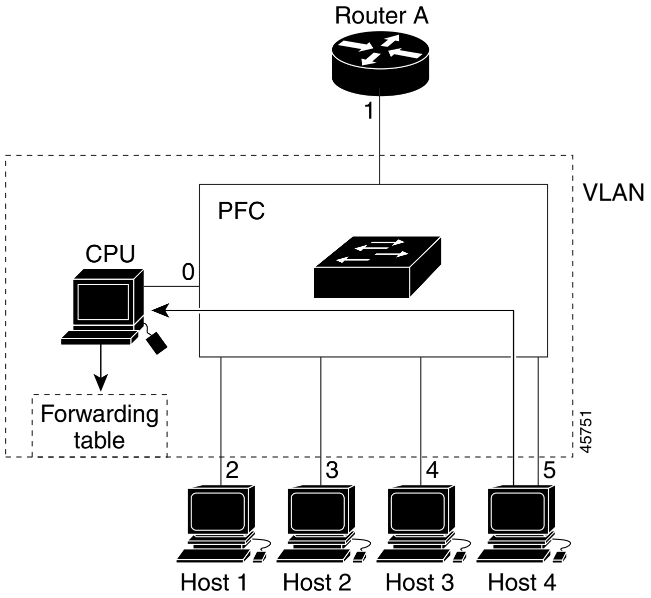


Table 25-1 IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports

Second Host Joining a Multicast Group



Updated IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports

Leaving a Multicast Group

Immediate Leave

Note

IGMP Configurable-Leave Timer

IGMP Report Suppression

Note

Configuring IGMP Snooping

-
- , page 25-7
- Setting the Snooping Method, page 25-8
- Configuring a Multicast Router Port, page 25-9
- Configuring a Host Statically to Join a Group, page 25-9
- Enabling IGMP Immediate Leave, page 25-10
- Configuring the IGMP Leave Timer, page 25-10
- Configuring TCN-Related Commands, page 25-11
- Configuring the IGMP Snooping Querier, page 25-13
- Disabling IGMP Report Suppression, page 25-15

Default IGMP Snooping Configuration

Table 25-3 Default IGMP Snooping Configuration

Feature	Default Setting

Default IGMP Snooping Configuration (continued)

Multicast router learning (snooping) method	PIM-DVMRP
IGMP snooping Immediate Leave	Disabled
Static groups	None configured
TCN[1] flood query count	2
TCN query solicitation	Disabled
IGMP snooping querier	Disabled
IGMP report suppression	Enabled

[1] TCN = Topology Change Notification

Enabling or Disabling IGMP Snooping

Beginning in privileged EXEC mode, follow these steps to globally enable IGMP snooping on the switch:

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To globally disable IGMP snooping on all VLAN interfaces, use the global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN interface:

	Enter global configuration mode.
	Enable IGMP snooping on the VLAN interface.The VLAN ID range is 1 to 1001 and 1006 to 4094. IGMP snooping must be globally enabled before you can enable VLAN snooping.
	Return to privileged EXEC mode.
	(Optional) Save your entries in the configuration file.

To disable IGMP snooping on a VLAN interface, use the global configuration command for the specified VLAN number

Setting the Snooping Method

-

-
-

Note

	{ | }	Enable IGMP snooping on a VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. Specify the multicast router learning method: —Listen for CGMP packets. This method is useful for reducing control traffic. —Snoop on IGMP queries and PIM-DVMRP packets. This is the default.
		Return to privileged EXEC mode.
	show ip igmp snooping	Verify the configuration.
Step 5		

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

	Command	Purpose
Step 1		
Step 2		• •
Step 3		
Step 4	[ ]	Verify that IGMP snooping is enabled on the VLAN interface.
		(Optional) Save your entries in the configuration file.

```
configure terminal
        ip igmp snooping vlan 200 mrouter interface gigabitethernet1/2
        end
```

Configuring a Host Statically to Join a Group

	Enter global configuration mode.
	Statically configure a Layer 2 port as a member of a multicast group: is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094. is the group IP address. is the member port. It can be a physical interface or a port channel (1 to 6).
	Return to privileged EXEC mode.

To remove the Layer 2 port from the multicast group, use the
global configuration command.

This example shows how to statically configure a host on a port:

```
ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/1
end
```

```
configure terminal
        ip igmp snooping vlan 130 immediate-leave
        end
```

- *might*

	Command	Purpose
Step 1		
Step 2		
Step 3		**Note**
Step 4		
Step 5		
Step 6		

last-member-query-interva

no ip igmp
snooping vlan **last-member-query-interval**

Configuring TCN-Related Commands

-
-
-

Controlling the Multicast Flooding Time After a TCN Event

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Recovering from Flood Mode

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Disabling Multicast Flooding During a TCN Event

exit	
show ip igmp snooping	
copy running-config startup-config	

Configuring the IGMP Snooping Querier

Beginning in privileged EXEC mode, follow these steps to enable the IGMP snooping querier feature in a VLAN:

Step 7		
Step 8		
Step 9		
Step 10		

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:

```
        ip igmp snooping querier 10.0.0.64
        end
```

```
configure terminal
        ip igmp snooping querier query-interval 25
        end
```

```
configure terminal
        ip igmp snooping querier timeout expiry 60
        end
```

```
configure terminal
        no ip igmp snooping querier version 2
        end
```

Disabling IGMP Report Suppression

Note

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Displaying IGMP Snooping Information

Table 25-4 Commands for Displaying IGMP Snooping Information

count |**dynamic** **count** | **user** **count**	**count** **dynamic** **user**

Command	Purpose
	• • • • •
	Note

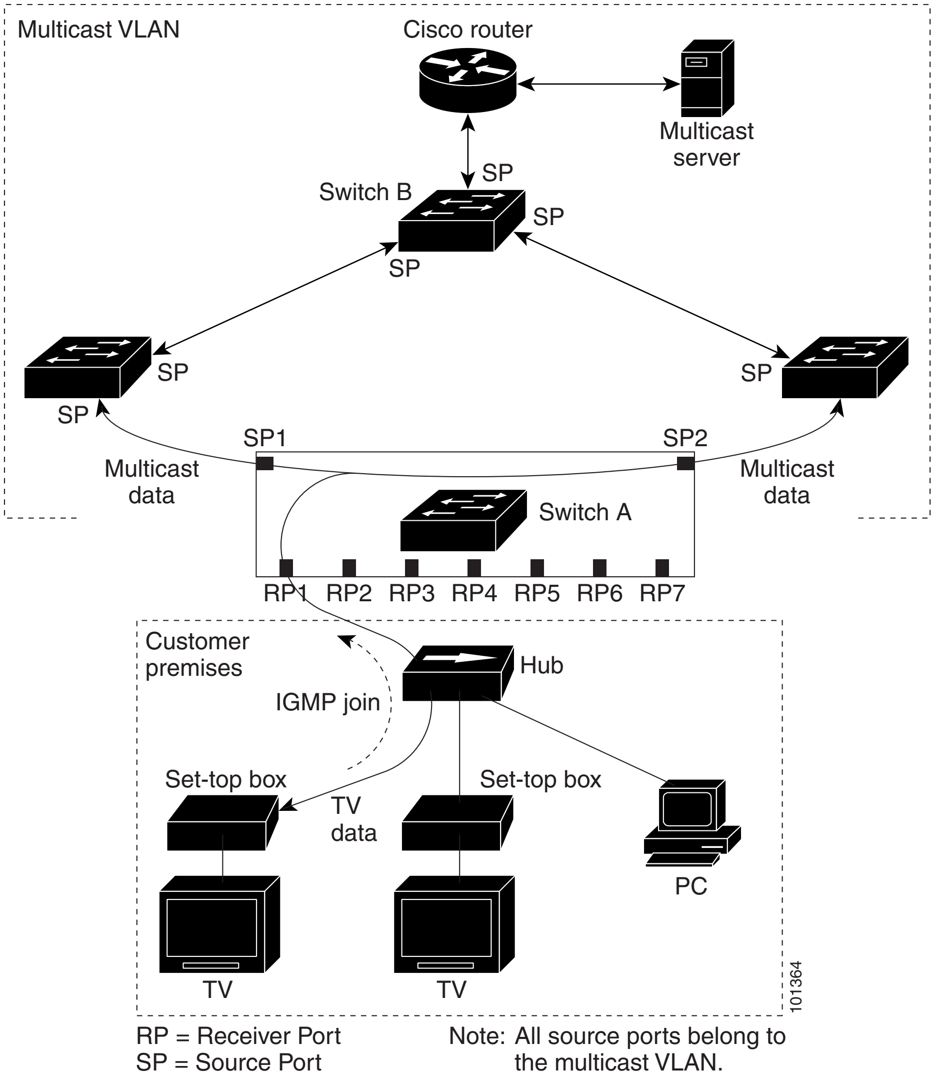
Understanding Multicast VLAN Registration

•

•

Using MVR in a Multicast Television Application

Multicast VLAN Registration Example



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, based on the MVR mode.

These sections contain this configuration information:

Default MVR Configuration, page 25-19

MVR Configuration Guidelines and Limitations, page 25-19

Configuring MVR Global Parameters, page 25-20

Configuring MVR Interfaces, page 25-21

Table 25-5 shows the default MVR configuration.

MVR	Disabled globally and per interface
Multicast addresses	None configured
Query response time	0.5 second
Multicast VLAN	VLAN 1
Mode	Compatible
Interface (per port) default	Neither a receiver nor a source port
Immediate Leave	Disabled on all ports

Follow these guidelines when configuring MVR:

Receiver ports can only be access ports; they cannot be trunk ports. Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.

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 256.

MVR multicast data received in the source VLAN and leaving from receiver ports has its time-to-live (TTL) decremented by 1 in the switch.

Because MVR on the switch uses IP multicast addresses instead of MAC multicast addresses, aliased IP multicast addresses are allowed on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).

MVR can coexist with IGMP snooping on a switch.

MVR data received on an MVR receiver port is not forwarded to MVR source ports.

MVR does not support IGMPv3 messages.

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

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

Beginning in privileged EXEC mode, follow these steps to configure MVR parameters:

	Enter global configuration mode.
	Enable MVR on the switch.
[ ]	Configure an IP multicast address on the switch or use the parameter to configure a contiguous series of MVR group addresses (the range for 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.
	(Optional) Define 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 5 tenths or one-half second.
	(Optional) Specify 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.
{ }	(Optional) Specify the MVR mode of operation: —Allows dynamic MVR membership on source ports. —Is compatible with Catalyst 3500 XL and Catalyst 2900 XL switches and does not support IGMP dynamic joins on source ports. The default is mode.
	Return to privileged EXEC mode.
or	Verify the configuration.
	(Optional) Save your entries in the configuration file.

To return the switch to its default settings, use the [| | |] global configuration commands.

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

```
mvr group 228.1.23.4
mvr querytime 10
mvr vlan 22
mvr mode dynamic
end
```

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

Beginning in privileged EXEC mode, follow these steps to configure Layer 2 MVR interfaces:

	Enter global configuration mode.
	Enable MVR on the switch.
	Specify the Layer 2 port to configure, and enter interface configuration mode.
{ | }	Configure an MVR port as one of these: —Configure 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. —Configure 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. The default configuration is as a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails.
[ ]	(Optional) Statically configure a port to receive multicast traffic sent to the multicast VLAN and the IP multicast address. A port statically configured as a member of a group remains a member of the group until statically removed. In compatible mode, this command applies to only receiver ports. In dynamic mode, it applies to receiver ports and source ports. Receiver ports can also dynamically join multicast groups by using IGMP join and leave messages.
	(Optional) Enable the Immediate-Leave feature of MVR on the port. This command applies to only receiver ports and should only be enabled on receiver ports to which a single receiver device is connected.
	Return to privileged EXEC mode.

To return the interface to its default settings, use the [| | |] interface configuration commands.

This example shows how to configure a port as a receiver port, statically configure the port to receive multicast traffic sent to the multicast group address, configure Immediate Leave on the port, and verify the results.

```
                mvr
                interface gigabitethernet1/2
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config)#
Switch# show mvr interface
Port    Type        Status          Immediate Leave
----    ----        -------         ---------------
Gi1/2   RECEIVER    ACTIVE/DOWN     ENABLED
```

Table 25-6 Commands for Displaying MVR Information

-id	

Command	Purpose

Configuring IGMP Filtering and Throttling

Note

-
-
-
-
-

Default IGMP Filtering and Throttling Configuration

Table 25-7 Default IGMP Filtering Configuration

Feature	Default Setting

Configuring IGMP Profiles

-
-
-
-
-

	Command	Purpose
Step 1		
Step 2	*profile number*	

profile number

ip multicast address

```
Switch(config-igmp-profile)#
Switch(config-igmp-profile)# range 229.9.9.0
                             end
        show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

```
Switch(config)#
Switch(config-if)#
Switch(config-if)#
```

Setting the Maximum Number of IGMP Groups

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

```
Switch(config)#
Switch(config-if)#
Switch(config-if)#
```

Configuring the IGMP Throttling Action

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

Displaying IGMP Filtering and Throttling Configuration

Table 25-8 Commands for Displaying IGMP Filtering and Throttling Configuration
