



Configuring IGMP Snooping and MVR

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on your switch, including an application of local IGMP snooping, Multicast VLAN Registration (MVR).



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release and the *Cisco IOS Release Network Protocols Command Reference, Part 1, for Release 12.1*.

This chapter consists of these sections:

- [Understanding IGMP Snooping, page 10-1](#)
- [Configuring IGMP Snooping, page 10-4](#)
- [Displaying IGMP Snooping Information, page 10-9](#)
- [Understanding Multicast VLAN Registration, page 10-12](#)



Note

For MAC addresses that map to IP multicast groups, you can either manage them through features such as IGMP snooping and MVR, or you can use static MAC addresses. However, you cannot use both methods simultaneously. Therefore, before using IGMP snooping or MVR, you should remove all statically configured MAC addresses that map to IP multicast groups.

Understanding IGMP Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated 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 deletes entries periodically if it does not receive IGMP membership reports from the multicast clients.



Note

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

The multicast router (which could be a Catalyst 3550 switch with the enhanced multilayer switch image) 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 forwards only one join request per IP multicast group to the multicast router. It creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request.

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

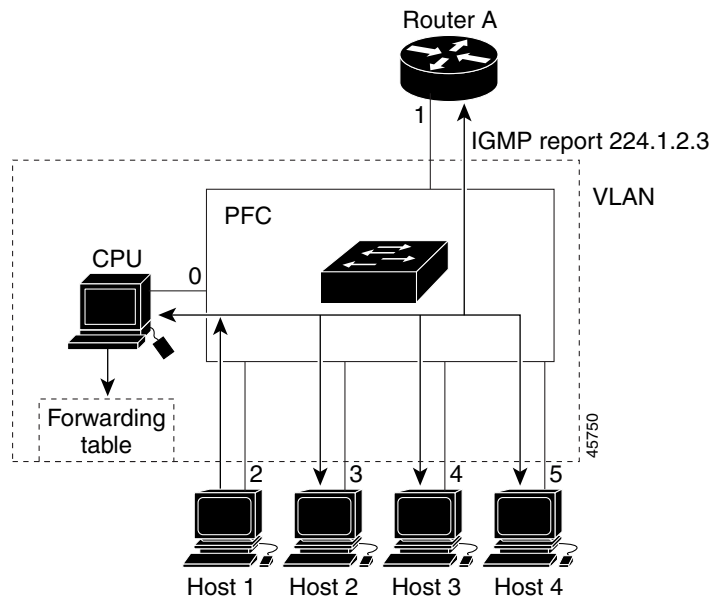
**Note**

If a spanning-tree VLAN topology change occurs, the IGMP snooping-learned multicast groups on the VLAN are purged. Enabling spanning-tree Port Fast on direct-to-desktop ports stops STP topology change notifications from being generated.

Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. Hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group. Refer to [Figure 10-1](#).

Figure 10-1 Initial IGMP Join Message



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 10-1](#), that includes the port numbers of Host 1, the router, and the switch internal CPU.

Table 10-1 IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2

Note that 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 IGMP packets only to the switch 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 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 10-2](#)), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in [Table 10-2](#). Note that because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the switch. Any multicast traffic is forwarded to the group and not to the CPU.

Figure 10-2 Second Host Joining a Multicast Group

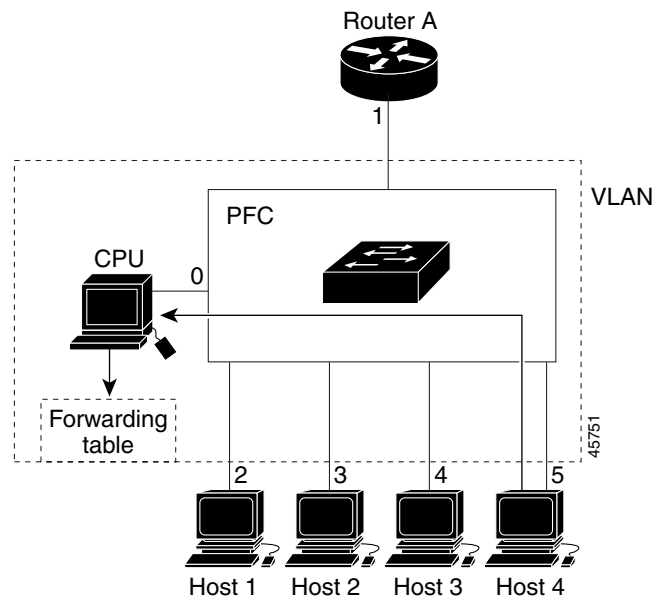


Table 10-2 Updated IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2, 5

Leaving a Multicast Group

The router sends periodic multicast general queries and the switch forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wishes to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The switch forwards multicast group traffic only to those hosts listed in the forwarding table for that Layer 2 multicast group.

When hosts want to leave a multicast group, they can either silently leave, or they can send a leave message. When the switch receives a 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. The switch then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

Immediate-Leave Processing

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

**Note**

You should use the Immediate-Leave processing feature only on VLANs where only one host is connected to each port. If Immediate-Leave is enabled in VLANs where more than one host is connected to a port, some hosts might be inadvertently dropped. Immediate Leave is supported only with IGMP version 2 hosts.

Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. To enable IGMP snooping on the switch to discover external multicast routers, the Layer 3 interfaces on the routers in the VLAN must already have been configured for multicast routing. For more information, see [Chapter 22, “Configuring IP Multicast Routing.”](#)

These sections describe how to configure IGMP snooping:

- [Default IGMP Snooping Configuration, page 10-5](#)
- [Enabling or Disabling IGMP Snooping, page 10-5](#)
- [Setting the Snooping Method, page 10-6](#)
- [Configuring a Multicast Router Port, page 10-7](#)
- [Configuring a Host Statically to Join a Group, page 10-7](#)
- [Enabling IGMP Immediate-Leave Processing, page 10-8](#)

Default IGMP Snooping Configuration

Table 10-3 shows the default IGMP snooping configuration.

Table 10-3 Default IGMP Snooping Configuration

Feature	Default Setting
IGMP snooping	Enabled globally and per VLAN
Multicast routers	None configured
Multicast router learning (snooping) method	PIM-DVMRP
IGMP snooping Immediate Leave	Disabled
Static groups	None configured

Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the switch. When enabled or disabled globally, it is also enabled or disabled in all existing VLAN interfaces. IGMP snooping is by default enabled on all VLANs, but can be enabled and disabled on a per-VLAN basis. After you configure the VLAN interface for multicast routing, no configuration is needed for the switch to access external multicast routers dynamically by using IGMP snooping.

Global IGMP snooping overrides the VLAN IGMP snooping. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable VLAN snooping.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip igmp snooping</code>	Globally enable IGMP snooping in all existing VLAN interfaces.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>copy running-config startup-config</code>	(Optional) Save your configuration to the startup configuration.

To globally disable IGMP snooping on all existing VLAN interfaces, use the **no ip igmp snooping** global configuration command.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip igmp snooping vlan <i>vlan-id</i></code>	Enable IGMP snooping on the VLAN interface.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>copy running-config startup-config</code>	(Optional) Save your configuration to the startup configuration.

To disable IGMP snooping on a VLAN interface, use the global configuration command **no ip igmp snooping vlan *vlan-id*** for the specified VLAN number.

Setting the Snooping Method

Multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns of such ports through one of these methods:

- Snooping on IGMP queries, Protocol Independent Multicast (PIM) packets, and Distance Vector Multicast Routing Protocol (DVMR) packets
- Listening to Cisco Group Management Protocol (CGMP) packets from other routers
- Statically connecting to a multicast router port with the **ip igmp snooping mrouter** command

You can configure the switch either to snoop on IGMP queries and PIM/DVMRP packets or to listen to CGMP self-join or proxy-join packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through only CGMP packets, use the **ip igmp snooping vlan *vlan-id* mrouter learn cgmp** global configuration mode command. When this command is issued, the router listens to CGMP self-join and CGMP proxy-join packets only and no other CGMP packets. To learn of multicast router ports through only PIM-DVMRP packets, use the **ip igmp snooping vlan *vlan-id* mrouter learn pim-dvmrp** interface mode command.



Note

If you want to use CGMP as the learning method and no multicast routers in the VLAN are CGMP proxy-enabled, you must enter the **ip cgmp router-only** command to dynamically access the router. For more information, see [Chapter 22, “Configuring IP Multicast Routing.”](#)

Beginning in privileged EXEC mode, follow these steps to alter the method in which a VLAN interface dynamically accesses a multicast router:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip igmp snooping vlan <i>vlan-id</i> mrouter learn <i>method</i>	The VLAN ID has a range of 1 to 1001. Specify the multicast router learning method: <ul style="list-style-type: none"> • cgmp to specify listening for CGMP packets. This method is useful for cutting down on control traffic. • pim-dvmrp to specify snooping IGMP queries and PIM-DVMRP packets.
Step 3	end	Return to privileged EXEC mode.
Step 4	show ip-igmp snooping	Verify the configuration.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
Switch# show ip igmp snooping vlan 1
vlan 1
-----
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 cgmp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

Configuring a Multicast Router Port

To add a multicast router port (add a static connection to a multicast router), use the **ip igmp snooping vlan mrouter** global configuration command on the switch.



Note

Static connections to multicast routers are supported only on switch ports.

Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	Specify the multicast router VLAN ID (1 to 1001), and specify the interface to the multicast router.
Step 3	end	Return to privileged EXEC mode.
Step 4	show ip igmp snooping mrouter [vlan <i>vlan-id</i>]	Verify that IGMP snooping is enabled on the VLAN interface.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config-if)# end

Switch# show ip igmp snooping mrouter vlan 200
vlan                ports
-----+-----
200                 Gi0/2
```

Configuring a Host Statically to Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode
Step 2	ip igmp snooping vlan <i>vlan-id</i> static <i>mac-address</i> interface <i>interface-id</i>	Statically configure a Layer 2 port as a member of a multicast group: <ul style="list-style-type: none"> <i>vlan-id</i> is the multicast group VLAN ID. <i>mac-address</i> is the group MAC address. <i>interface-id</i> is the member port.
Step 3	end	Return to privileged EXEC mode.

	Command	Purpose
Step 4	show ip igmp snooping mrouter vlan <i>vlan-id</i>	Verify that the member port is a member of the VLAN multicast group.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to statically configure a host on an interface:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 4 static 0100.5e02.0203 interface
gigabitethernet0/11
Configuring port Gigabit Ethernet0/11 on group 0100.5e02.0203 vlan 4
Switch(config)# end
Switch #
Switch# show ip igmp snooping mrouter vlan 4
vlan          ports
-----+-----
4             Gi 0/11
```

Enabling IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.

Immediate Leave is supported only with IGMP version 2 hosts.

Beginning in privileged EXEC mode, follow these steps to enable IGMP Immediate-Leave processing:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode
Step 2	ip igmp snooping vlan <i>vlan-id</i> immediate-leave	Enable IGMP Immediate-Leave processing on the VLAN interface.
Step 3	end	Return to privileged EXEC mode.
Step 4	show ip igmp snooping vlan <i>vlan-id</i>	Verify that Immediate Leave is enabled on the VLAN.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to enable IGMP immediate-leave processing and verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 immediate-leave
Configuring immediate leave on vlan 1
Switch(config)# end
Switch#
```

To disable Immediate-Leave processing, use the **no ip igmp snooping vlan** *vlan-id* **immediate-leave** command.

Displaying IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

Viewing Snooping Configuration

You can display snooping configuration information for the switch or for a specified VLAN.

Beginning in privileged EXEC mode, use this command to display snooping configuration:

Command	Purpose
<code>show ip igmp snooping [vlan <i>vlan-id</i>]</code>	Display snooping configuration. (Optional) <i>vlan-id</i> is the number of the VLAN.

This example shows how to display snooping information for all VLAN interfaces on the switch:

```
Switch# show ip igmp snooping
vlan 1
-----
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
vlan 2
-----
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
vlan 10
-----
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
vlan 11
-----
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
vlan 12
-----
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
```

This example shows how to display snooping information for a specific VLAN interface:

```
Switch# show ip igmp snooping vlan 1
vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping is disabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

Viewing Multicast Router Interfaces

When you enable IGMP snooping, the switch automatically learns to which interface a multicast router is connected.

Beginning in privileged EXEC mode, use this command to display the statically and dynamically learned multicast router ports:

Command	Purpose
<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	Display information on dynamically learned and manually configured multicast router interfaces.

This example shows how to display information on all multicast router interfaces on the switch:

```
Switch# show ip igmp snooping mrouter
vlan          ports
-----+-----
1             Gi0/1,Gi0/2,Router
2             Gi0/3,Gi0/4
```

This example shows how to display information on all multicast router ports on VLAN 1:

```
Switch# show ip igmp snooping mrouter vlan 1
Vlan  ports
----  -----
1     Gi0/1(dynamic)
1     Gi0/2(dynamic)
```

You can also use the `show mac-address-table multicast [vlan vlan-id]` command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

Viewing MAC Address Multicast Entries

You can view the Layer 2 MAC address multicast entries for a VLAN configured for IGMP snooping. Beginning in privileged EXEC mode, use this command to display the Layer 2 multicast information:

Command	Purpose
show mac-address-table multicast [vlan <i>vlan-id</i>] [user igmp-snooping] [count]	Display MAC address table entries for a VLAN. <ul style="list-style-type: none"> (Optional) vlan <i>vlan-id</i> is the multicast group VLAN ID. (Optional) user displays only the user-configured multicast entries. (Optional) igmp-snooping displays entries learned through IGMP snooping. (Optional) count displays only the total number of entries for the selected criteria, not the actual entries.

This example shows how to display the Layer 2 multicast entries for VLAN 1:

```
Switch# show mac-address-table multicast vlan 1
vlan  mac address      type      ports
-----+-----+-----+-----
  1  0100.5e02.0203    user      Gi0/1,Gi0/2
  1  0100.5e00.0127    igmp      Gi0/1,Gi0/2
  1  0100.5e00.0128    user      Gi0/1,Gi0/2
  1  0100.5e00.0001    igmp      Gi0/1,Gi0/2
```

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

```
Switch# show mac-address-table multicast count

Multicast MAC Entries for all vlans:    10
```

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:
```

This example shows how to display only the user-configured multicast entries for VLAN 1:

```
Switch# show mac-address-table multicast vlan 1 user
vlan  mac address      type      ports
-----+-----+-----+-----
  1  0100.5e02.0203    user      Gi0/1,Gi0/2
  1  0100.5e00.0128    user      Gi0/1,Gi0/2
```

This example shows how to display the total number of entries learned by IGMP snooping for VLAN 1:

```
Switch# show mac-address-table multicast vlan 1 igmp-snooping count

Number of user programmed entries:    2
```

Understanding Multicast VLAN Registration

Multicast VLAN Registration (MVR) is designed for applications using 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 can be enabled or disabled without affecting the behavior of the other feature. However, if IGMP snooping and MVR are both enabled, MVR only reacts 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.

The switch CPU identifies the MVR IP multicast streams and their associated MAC addresses in the switch forwarding table, intercepts the IGMP messages, and modifies the 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 the two VLANs.

The Catalyst 3550 switch has two modes of MVR operation: dynamic mode and compatible mode.

- When operating in MVR dynamic mode, the switch performs standard IGMP snooping. IGMP information packets are sent to the switch CPU, but multicast data packets are not sent to the CPU. Dynamic mode allows the multicast router to run normally because the switch sends the IGMP join messages to the router, and the router only forwards multicast streams for a particular group to an interface if it has received a join message from the interface for the group. Receiver ports are treated as members of the multicast VLAN for MVR multicast control and data traffic. IGMP reports for MVR groups are sent out source ports in the multicast VLAN.



Note Unknown unicast and broadcast traffic in the multicast VLAN are leaked to ports outside the VLAN boundary.

- MVR compatible mode of operation supports MVR interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches. It works the same as dynamic mode for all multicast data packets and IGMP query and leave packets. However, received IGMP report packets for MVR groups are not sent out on the multicast VLAN source ports. In contrast to dynamic mode, the switch does not send join messages to the router. The router must be statically configured for the interface to receive the multicast stream. Therefore, in this mode, MVR does not support dynamic membership joins on source ports.

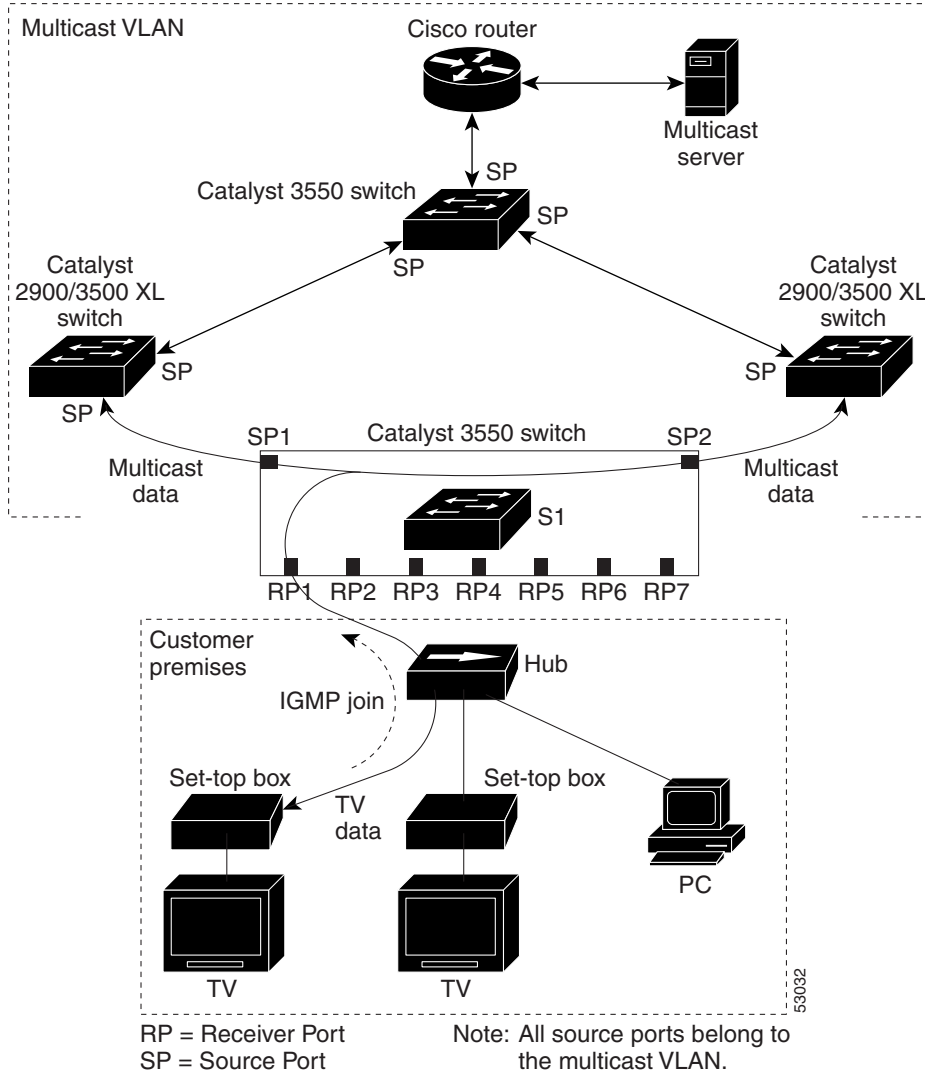
Using MVR in a Multicast Television Application

In a multicast TV 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. Refer to [Figure 10-3](#). 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 the S1 switch to join the appropriate multicast. If the IGMP report matches one of the configured multicast MAC addresses, the switch 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.

When a subscriber changes channels or turns off the TV, the set-top box sends an IGMP leave message for the multicast stream. The switch CPU sends an IGMP group-specific 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. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

If the Immediate-Leave feature is enabled on a receiver port, the port leaves a multicast group more quickly. Without Immediate Leave, 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 Immediate Leave, 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. The Immediate Leave feature should only be enabled on receiver ports to which a single receiver device is connected.

Figure 10-3 Multicast VLAN Registration Example



MVR eliminates the need to duplicate TV-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only once around the VLAN trunk—only on the multicast VLAN. Although the IGMP leave and join messages originate with a subscriber, they appear to be initiated by a port in the multicast VLAN rather than 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. The access layer switch (S1 switch) 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 MAC addresses as the multicast data. The S1 CPU must capture all IGMP join and leave messages from receiver ports and forward them to the multicast VLAN of the source (uplink) port.

Configuration Guidelines and Limitations

Follow these guidelines when configuring MVR:

- Receiver ports 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 that can be configured on a switch (that is, the maximum number of television channels that can be received) is 256.
- Each channel is one multicast stream destined for a unique IP multicast address. These IP addresses cannot alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xx).
- Multicast routing and MVR cannot coexist on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled, and you receive a warning message. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled, and you receive an Error message.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

Default MVR Configuration

Table 10-4 shows the default MVR configuration.

Table 10-4 Default MVR Configuration

Feature	Default Setting
MVR	Disabled globally and per interface
Multicast addresses	None configured
Group IP address count	1
Query response time	0.5 second
Multicast VLAN	VLAN 1
Mode	Compatibility
Interface (per port) default	Neither a receiver or source port
Immediate Leave	Disabled on all ports

Configuring MVR Global Parameters

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.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>mvr</code>	Enable MVR on the switch.
Step 3	<code>mvr group ip-address [count]</code>	<p>Configure an IP multicast address on the switch or use the <i>count</i> parameter to configure a contiguous series of IP addresses. 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 TV channel.</p> <p>Note Each IP address translates to a multicast 48-bit MAC address. If an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses, the command fails.</p>
Step 4	<code>mvr querytime value</code>	(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 default is 5 tenths or one-half of a second.
Step 5	<code>mvr vlan vlan-id</code>	(Optional) Specify the VLAN in which multicast data will be received; all source ports must belong to this VLAN. The VLAN range is 1 to 1001. The default is VLAN 1.
Step 6	<code>mvr mode {dynamic compatible}</code>	<p>(Optional) Specify the MVR mode of operation:</p> <ul style="list-style-type: none"> dynamic mode allows dynamic MVR membership on source ports. compatible mode provides for compatibility with Catalyst 2900 XL and Catalyst 3500 XL switches and does not support IGMP dynamic joins on source ports. <p>The default is compatible mode.</p>
Step 7	<code>end</code>	Exit configuration mode.
Step 8	<code>show mvr</code> <code>show mvr members</code>	Verify the configuration.
Step 9	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
Switch# show mvr
MVR Running: TRUE
MVR multicast vlan: 22
MVR Max Multicast Groups: 256
MVR Current multicast groups: 256
MVR Global query response time: 10 (tenths of sec)
MVR Mode: dynamic
```

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

Configuring MVR Interfaces

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	mvr	Enable MVR on the switch.
Step 3	interface <i>interface-id</i>	Enter interface configuration mode, and enter the type and number of the port to configure, for example, gi 0/1 or gigabitethernet 0/1 for Gigabit Ethernet port 1.
Step 4	mvr type { source receiver }	Configure an MVR port as one of these: <ul style="list-style-type: none"> • source—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. • receiver —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.
Step 5	mvr vlan <i>vlan-id</i> group <i>ip-address</i>	(Optional) Statically configure a port to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of a group remains a member of the group until statically removed. <p>Note In compatible mode, this command applies only to receiver ports. In dynamic mode, it applies to receiver ports and source ports.</p> <p>Receiver ports can also dynamically join multicast groups by using IGMP join and leave messages.</p>

	Command	Purpose
Step 6	mvr immediate	(Optional) Enable the Immediate Leave feature of MVR on the port. Note This command applies only to receiver ports and should only be enabled on receiver ports to which a single receiver device is connected.
Step 7	end	Exit configuration mode.
Step 8	show mvr show mvr interface show mvr members	Verify the configuration.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure Gigabit Ethernet port 0/1 as a receiver port, statically configure the port to receive multicast traffic sent to the multicast group address, configure Immediate Leave on the interface, and verify the results.

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: ENABLED
```

This example shows the results of the **show mvr interface** privileged EXEC command when the **member** keyword is included:

```
Switch# show mvr interface gigabitethernet0/6 member
239.255.0.0    DYNAMIC ACTIVE
239.255.0.1    DYNAMIC ACTIVE
239.255.0.2    DYNAMIC ACTIVE
239.255.0.3    DYNAMIC ACTIVE
239.255.0.4    DYNAMIC ACTIVE
239.255.0.5    DYNAMIC ACTIVE
239.255.0.6    DYNAMIC ACTIVE
239.255.0.7    DYNAMIC ACTIVE
239.255.0.8    DYNAMIC ACTIVE
239.255.0.9    DYNAMIC ACTIVE
```

Displaying MVR

You can display MVR information for the switch or for a specified interfaces.

Beginning in privileged EXEC mode, use the commands in [Table 10-4](#) to display MVR configuration:

Table 10-5 Commands for Displaying MVR Information

<code>show mvr</code>	Displays MVR status and values for the switch—whether MVR is enabled or disabled, the multicast VLAN, the number of multicast groups (always 256 for the Catalyst 3550 switch), the query response time, and the MVR mode.
<code>show mvr interface [interface-id] [members [vlan vlan-id]]</code>	<p>Displays all MVR interfaces and their MVR configurations.</p> <p>When a specific interface is entered, displays this information:</p> <ul style="list-style-type: none"> • Type—Receiver or Source • Status—One of these: <ul style="list-style-type: none"> – Active means the port is part of a VLAN. – Up/Down means that the port is forwarding or nonforwarding. – Inactive means that the port is not yet part of any VLAN. • Immediate Leave—Enabled or Disabled <p>If the members keyword is entered, displays all multicast group members on this port or, if a VLAN identification is entered, all multicast group members on the VLAN.</p>
<code>show mvr members [ip-address]</code>	Displays all receiver ports that are members of any IP multicast group or the specified IP multicast group IP address.

This example shows the results of the `show mvr` privileged EXEC command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast vlan: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 256
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

This example shows the results of the `show mvr interface` privileged EXEC command:

```
Switch# show mvr interface
Port      Type      Status      Immediate Leave
----      -
Gi0/1     SOURCE    ACTIVE/UP   DISABLED
Gi0/2     SOURCE    ACTIVE/UP   DISABLED
Gi0/3     RECEIVER  ACTIVE/UP   DISABLED
Gi0/4     RECEIVER  ACTIVE/UP   DISABLED
Gi0/5     RECEIVER  ACTIVE/UP   ENABLED
Gi0/6     RECEIVER  ACTIVE/UP   DISABLED
Gi0/7     RECEIVER  ACTIVE/UP   ENABLED
Gi0/8     RECEIVER  ACTIVE/UP   DISABLED
```

This example shows the results of the `show mvr interface` privileged EXEC command for a specified interface:

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This example shows the results of the **show mvr interface** privileged EXEC command when the **member** keyword is included:

```
Switch# show mvr interface gigabitethernet0/6 member
239.255.0.0      DYNAMIC ACTIVE
239.255.0.1      DYNAMIC ACTIVE
239.255.0.2      DYNAMIC ACTIVE
239.255.0.3      DYNAMIC ACTIVE
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

This example shows the results of the **show mvr member** privileged EXEC command:

```
Switch# show mvr member
MVR Group IP      Status           Members
-----
239.255.0.1      ACTIVE          Gi0/1(d), Gi0/5(s)
239.255.0.2      INACTIVE       None
239.255.0.3      INACTIVE       None
239.255.0.4      INACTIVE       None
239.255.0.5      INACTIVE       None
239.255.0.6      INACTIVE       None
239.255.0.7      INACTIVE       None
239.255.0.8      INACTIVE       None
239.255.0.9      INACTIVE       None
239.255.0.10     INACTIVE       None

<output truncated>

239.255.0.255    INACTIVE       None
239.255.1.0      INACTIVE       None
```