

Table of Contents

Chapter 1 IGMP Snooping Configuration	1-1
1.1 Introduction	1-1
1.1.1 IGMP Snooping Fundamentals	1-1
1.1.2 IGMP Snooping Implementation	1-2
1.2 IGMP Snooping Configuration	1-5
1.2.1 Enabling IGMP Snooping.....	1-5
1.2.2 Configuring Timers	1-6
1.2.3 Enabling IGMP Fast Leave Processing	1-7
1.2.4 Configuring IGMP Snooping Filter ACL	1-7
1.2.5 Configuring the Maximum Number of Multicast Groups on a Port	1-8
1.2.6 Configuring Multicast VLAN	1-9
1.3 Displaying Information about IGMP Snooping.....	1-11
1.4 IGMP Snooping Configuration Examples	1-11
1.4.1 Example 1	1-11
1.4.2 Example 2	1-12
1.5 Troubleshooting IGMP Snooping.....	1-15
Chapter 2 IGMP Group Limit on Interface.....	2-1
2.1 Introduction	2-1
2.1.1 Configuring the Maximum Number of IGMP Groups on an Interface	2-1
Chapter 3 Multicast MAC Address Entry Configuration.....	3-1
3.1 Introduction	3-1
3.2 Multicast MAC Address Entry Configuration	3-1
3.3 Displaying Multicast MAC Address Configuration	3-2
Chapter 4 Multicast Source Deny Configuration	4-1
4.1 Introduction	4-1
4.2 Enabling Multicast Source Deny.....	4-1
4.3 Displaying Multicast Source Deny Configuration.....	4-1
Chapter 5 IGMP Snooping Configuration Commands.....	5-1
5.1 IGMP Snooping Configuration Commands	5-1
5.1.1 display igmp-snooping configuration.....	5-1
5.1.2 display igmp-snooping group	5-2
5.1.3 display igmp-snooping statistics.....	5-3
5.1.4 igmp-snooping.....	5-4
5.1.5 igmp-snooping fast-leave	5-4
5.1.6 igmp-snooping group-limit.....	5-5
5.1.7 igmp-snooping group-policy	5-6

5.1.8 igmp-snooping host-aging-time.....	5-8
5.1.9 igmp-snooping max-response-time.....	5-8
5.1.10 igmp-snooping router-aging-time	5-9
5.1.11 reset igmp-snooping statistics.....	5-10
5.1.12 service-type multicast.....	5-10
Chapter 6 IGMP Group Limit Commands.....	6-1
6.1 IGMP Group Limit Commands.....	6-1
6.1.1 igmp group-limit.....	6-1
Chapter 7 Multicast MAC Address Entry Configuration Commands.....	7-1
7.1 Multicast MAC Address Entry Configuration Commands.....	7-1
7.1.1 mac-address multicast interface vlan.....	7-1
7.1.2 mac-address multicast vlan.....	7-2
7.1.3 display mac-address multicast static.....	7-2
Chapter 8 Multicast Source Deny Commands	8-1
8.1 Multicast Source Deny Commands	8-1
8.1.1 multicast-source-deny	8-1
8.1.2 display multicast-source-deny.....	8-2

Chapter 1 IGMP Snooping Configuration

1.1 Introduction

1.1.1 IGMP Snooping Fundamentals

IGMP Snooping (internet group management protocol snooping) is a multicast control mechanism running on Layer 2 switches. It is used to manage and control multicast groups.

When the IGMP messages transferred from the hosts to the router pass through the Layer 2 switch, the switch uses IGMP Snooping to analyze and process the information carried in the IGMP messages.

Table 1-1 IGMP messages processing on the switch

Message type	Sender	Receiver	Processing on the switch
IGMP host report message	Host	Switch	Add the host to the corresponding multicast group.
IGMP leave message	Host	Switch	Remove the host from the multicast group.

By listening to IGMP messages, the switch establishes and maintains MAC multicast address tables at data link layer, and uses the tables to forward the multicast packets delivered from the router.

As shown in [Figure 1-1](#), multicast packets are broadcasted at Layer 2 when IGMP Snooping is disabled and multicasted (not broadcasted) at Layer 2 when IGMP Snooping is enabled.

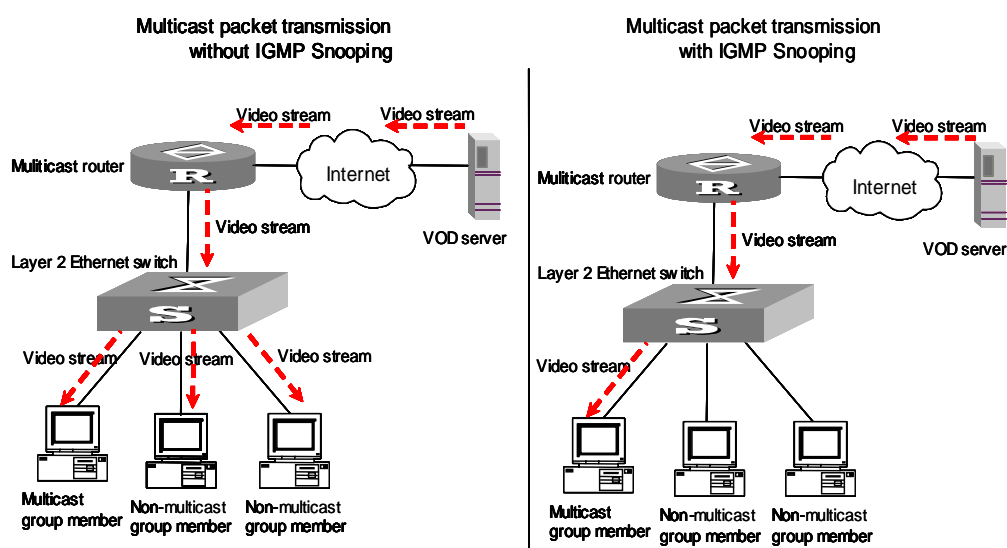


Figure 1-1 Multicast packet transmission with or without IGMP Snooping

1.1.2 IGMP Snooping Implementation

I. IGMP Snooping terminologies

Before going on, we first describe the following terms involved in IGMP Snooping:

- Router port: the port on the switch directly connected to the multicast router.
- Multicast member port: a port on the switch connected to a multicast group member. A multicast group member is a host that has joined a multicast group.
- MAC multicast group: a multicast group identified with a MAC multicast address and maintained by the switch.

The following three timers are closely associated with IGMP Snooping.

Table 1-2 Timers associated with IGMP Snooping

Timer	Set	Message normally received before timeout	Timeout action on the switch
Router port aging timer	Aging time of the router port	IGMP general query message	Consider that this port is not a router port any more.
Multicast member port aging timer	Aging time of the multicast member ports	IGMP message/PIM message/DVMRP Probe message	Send an IGMP group-specific query message to the multicast member port.
Query response timer	Maximum query response time	IGMP message report	Remove the port from the member port list of the multicast group.

II. Layer 2 multicast with IGMP Snooping

The switch runs IGMP Snooping to listen to IGMP messages and map the hosts and the corresponding ports to the corresponding multicast group addresses.

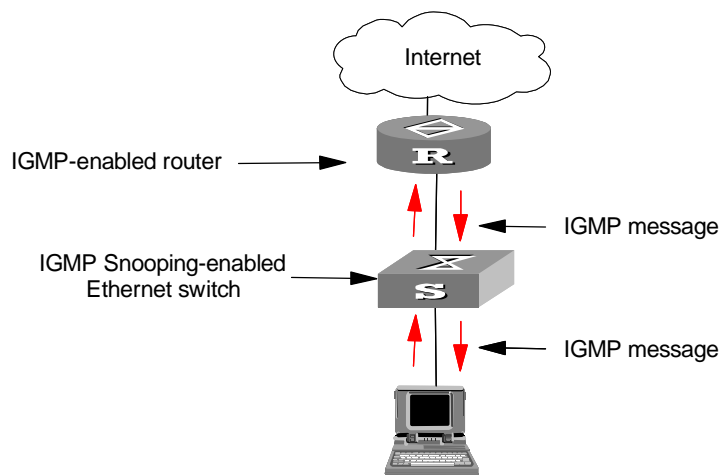


Figure 1-2 IGMP Snooping implementation

To implement Layer 2 multicast, the switch processes four different types of IGMP messages it receives as shown in [Table 1-3](#).

Table 1-3 Four types of IGMP messages

Message	Sender	Receiver	Purpose	Switch action	
IGMP general query message	Multicast router	Multicast member switch	Query if the multicast groups contain any member	Check if the message comes from the original router port	If yes, reset the aging timer of the router port.
					If not, notify the multicast router that a member is ready to join a multicast group and starts the aging timer for the router port.
IGMP group-specific query message	Multicast router	Multicast member switch	Query if a specific multicast group contains any member	Send a group-specific query message to the IP multicast group being queried.	

Message	Sender	Receiver	Purpose	Switch action		
IGMP host report message	Host	Multicast router	Apply for joining a multicast group, or responds to an IGMP query message	Check if the MAC multicast group corresponding to the IP multicast group exists.	If yes, check if the port exists in the MAC multicast group.	If yes, reset the aging timer of the port.
						If not, add the port to the MAC multicast group, resets the aging timer of the port and checks if the corresponding IP multicast group exists.
					If yes, add the port to the IP multicast group. If not, create an IP multicast group and adds the port to it. If not, Create a MAC multicast group and notifies the multicast router that a member is ready to join the multicast group. Add the port to the MAC multicast group and starts the aging timer of the port. Add all ports in the VLAN owning this port to the forward port list of the MAC multicast group. Add the port to the IP multicast group.	

Message	Sender	Receiver	Purpose	Switch action	
IGMP leave message	Host	Multicast router	Notify the multicast router that the host is leaving its multicast group.	Send group-specific query message to the multicast group of the port receiving the leave message to check if the multicast group has any member, and starts the corresponding query response timer.	<div>If no response is received from the port before the timer times out, remove the port from the corresponding MAC multicast group.</div> <div>If no response is received from the multicast group before the timer times out, notify the router to remove this multicast group node from the multicast tree.</div>



Note:

If IGMP Snooping is enabled on an S5600 series Ethernet switch, upon receiving an IGMP leave message from a host in a multicast group, the switch automatically judge whether the group exists or not. If the group does not exist, the switch discards the IGMP leave message without forwarding it to the router.

1.2 IGMP Snooping Configuration

The following sections describe the IGMP Snooping configuration tasks.

- [Enabling IGMP Snooping](#)
- [Configuring Timers](#)
- [Enabling IGMP Fast Leave Processing](#)
- [Configuring IGMP Snooping Filter ACL](#)
- [Configuring Multicast VLAN](#)

Except for the first one, all the other configuration tasks are optional (you can determine whether or not to perform these tasks according to your needs).

1.2.1 Enabling IGMP Snooping

You can use the command here to enable IGMP Snooping so that it can establish and maintain MAC multicast forwarding tables at layer 2.

Table 1-4 Enable IGMP Snooping

Operation	Command	Description
Enter system view	system-view	—
Enable IGMP Snooping globally	igmp-snooping enable	Required By default, IGMP Snooping is disabled globally.
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable IGMP Snooping on the VLAN	igmp-snooping enable	Required By default, IGMP Snooping is disabled on the VLAN.

**Caution:**

- Although both Layer 2 and Layer 3 multicast protocols can run on the same switch simultaneously, they cannot run simultaneously on a VLAN and its corresponding VLAN interface.
- IGMP Snooping functions on a VLAN only when it is first enabled globally in system view and then enabled in the VLAN view.

1.2.2 Configuring Timers

This configuration task is to manually configure the aging time of the router port, the aging time of the multicast member ports, and the maximum query response time.

- If the switch receives no general query message from a router within the aging time of the router port, the switch removes the router port from the port member lists of all MAC multicast groups.
- If the switch receives no IGMP report message within the aging time of a member port, it transmits a group-specific query message to the port and starts the query response timer of the IP multicast group.
- If the switch receives no IGMP report message within the maximum query response time, it removes the port from the member port list of the multicast group.

Table 1-5 Configure timers

Operation	Command	Description
Enter system view	system-view	—
Configure the aging time of the router port	igmp-snooping router-aging-time <i>seconds</i>	Optional By default, the aging time of the router port is 105 seconds.
Configure the aging time of multicast member ports	igmp-snooping host-aging-time <i>seconds</i>	Optional By default, the aging time of multicast member ports is 260 seconds.
Configure the maximum query response time	igmp-snooping max-response-time <i>seconds</i>	Optional By default, the maximum response time is 10 seconds.

1.2.3 Enabling IGMP Fast Leave Processing

Normally, when receiving an IGMP Leave message, IGMP Snooping does not immediately remove the port from the multicast group, but sends a group-specific query message. If no response is received in a given period, it then removes the port from the multicast group.

If IGMP fast leave processing is enabled, when receiving an IGMP Leave message, IGMP Snooping immediately removes the port from the multicast group. When a port has only one user, enabling IGMP fast leave processing on the port can save bandwidth.

Table 1-6 Enable IGMP fast leave processing

Operation	Command	Description
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable IGMP fast leave processing	igmp-snooping fast-leave vlan <i>vlan-id</i> [to <i>vlan-id</i>]	Required By default this function is disabled.

1.2.4 Configuring IGMP Snooping Filter ACL

You can configure multicast filter ACLs globally or on switch ports to use the IGMP Snooping filter function to limit the multicast programs that the users can order. With this function, you can treat different VoD users in different ways by allowing different users to order different groups of programs.

In practice, when a user orders a multicast program, an IGMP report message is generated. When the message arrives at the switch, the switch examines the multicast filter ACL referenced on the access port to determine if the port can join the corresponding multicast group or not. If yes, it adds the port to the forward port list of the multicast group. If not, it drops the IGMP report message and does not forward the corresponding data stream to the port. In this way, you can control the multicast programs that users can order.

Table 1-7 Configure IGMP Snooping filter ACL

Operation	Command	Description
Enter system view	system-view	—
Enable IGMP Snooping filter in system view	igmp-snooping group-policy <i>acl-number</i> vlan <i>vlan-list</i>	Required <i>acl-number</i> is the number of a basic ACL; <i>vlan-id</i> is a VLAN ID. By default, this function is not enabled.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure an IGMP Snooping filter ACL on the port	igmp-snooping group-policy <i>acl-number</i> vlan <i>vlan-list</i>	Required <i>acl-number</i> is the number of a basic ACL; <i>vlan-id</i> is a VLAN ID. By default, no ACL is configured on any port.

1.2.5 Configuring the Maximum Number of Multicast Groups on a Port

You can use the command here to limit the number of multicast groups on a switch port. After that, users on this port cannot unlimitedly order multicast programs because you have limited the number of multicast groups on this port. In this way, you can control the multicast bandwidth on a port.

Table 1-8 Configure the maximum number of multicast groups on a port

Operation	Command	Description
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the maximum number of multicast groups the port can join.	igmp-snooping group-limit [<i>vlan</i> <i>vlan-list</i>] overflow-replace	Required By default, there is no limit on the number of the multicast groups the port can join.

1.2.6 Configuring Multicast VLAN

In old multicast mode, when users in different VLANs order the same multicast group, the multicast stream is copied to each of the VLANs. This mode wastes a lot of bandwidth.

By configuring a multicast VLAN, adding switch ports to the multicast VLAN and enabling IGMP Snooping, you can make users in different VLANs share the same multicast VLAN. This saves bandwidth since multicast streams are transmitted only within the multicast VLAN, and also guarantees security because the multicast VLAN is isolated from user VLANs.

Multicast VLAN is mainly used in Layer 2 switching, but you must make corresponding configuration on the Layer 3 switch.

The following table describes the configuration tasks for multicast VLAN.

Table 1-9 Configure multicast VLAN on Layer 3 switch

Operation	Command	Description
Enter system view	system-view	—
Create a VLAN and enter the VLAN view	vlan <i>vlan-id</i>	<i>vlan-id</i> is a VLAN ID.
Exit the VLAN view	quit	—
Create a VLAN interface and enter the VLAN interface view	interface vlan-interface <i>vlan-id</i>	—
Enable IGMP	igmp enable	Required
Exit the VLAN interface view	quit	—
Enter the view of the Ethernet port connected to the Layer 2 switch	interface <i>interface-type</i> <i>interface-num</i>	—
Define the port as a trunk or hybrid port	port link-type { trunk hybrid }	Required
Set the VLAN IDs allowed to pass through the Ethernet	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	Required The multicast VLAN defined on the Layer 2 switch must be included and set as tagged.
	port trunk pvid vlan <i>vlan-id</i>	

Table 1-10 Configure multicast VLAN on Layer 2 switch

Operation	Command	Description
Enter system view	system-view	—
Enable IGMP Snooping globally	igmp-snooping enable	Required
Enter VLAN view	vlan <i>vlan-id</i>	<i>vlan-id</i> is a VLAN ID.
Enable IGMP Snooping on the VLAN	igmp-snooping enable	Required
Enable multicast VLAN	service-type multicast	Required
Exit the VLAN view	quit	—
Enter the view of the Ethernet port connected to the Layer 3 switch	interface <i>interface-type</i> <i>interface-num</i>	—
Define the port as a trunk or hybrid port	port link-type { trunk hybrid }	—
Set the VLAN IDs allowed to pass through the Ethernet	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	The multicast VLAN must be included and set as tagged.
	port trunk pvid <i>vlan</i> <i>vlan-id</i>	
Exit the current view	quit	—
Enter the view of the Ethernet port connected to a user device	interface <i>interface-type</i> <i>interface-num</i>	<i>interface-type</i> and <i>interface-num</i> are the interface type and interface number.
Define the port as a hybrid port	port link-type hybrid	Required
Set the VLAN IDs whose packets are allowed to pass the port	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	Required The multicast VLAN must be included and set as untagged.

Note:

- You cannot set the isolate VLAN as a multicast VLAN.
- One user port can belong to only one multicast VLAN.
- The port connected to a user end can only be set as a hybrid port.
- A multicast member port must belong to the same multicast VLAN with the router port. Or else, it cannot receive multicast packets.
- When setting a multicast VLAN ID on the router port, you must define the port as a trunk port or a tag-carried hybrid port, or else no multicast member port in this multicast VLAN can receive multicast packets.
- If a multicast member port needs to receive multicast packets forwarded by the router port but the router port does not belong to any multicast VLAN, you should remove the multicast member port from its multicast VLAN, or else it cannot receive multicast packets.

1.3 Displaying Information about IGMP Snooping

You can execute the following **display** commands in any view to display information about IGMP Snooping.

Table 1-11 Display IGMP Snooping

Operation	Command	Description
Display the current configuration information about IGMP Snooping	display igmp-snooping configuration	You can execute the display commands in any view.
Display the message statistics about IGMP Snooping	display igmp-snooping statistics	
Display information about the IP multicast groups and MAC multicast groups under one or all VLANs	display igmp-snooping group [vlan <i>vlanid</i>]	
Clear IGMP Snooping statistics	reset igmp-snooping statistics	You can execute the reset command in user view.

1.4 IGMP Snooping Configuration Examples

1.4.1 Example 1

Configure IGMP Snooping on a switch.

I. Network requirements

Connect the router port on the switch to the router, and other non-router ports which belong to VLAN 10 to user PCs. Enable IGMP Snooping on the switch.

II. Network diagram

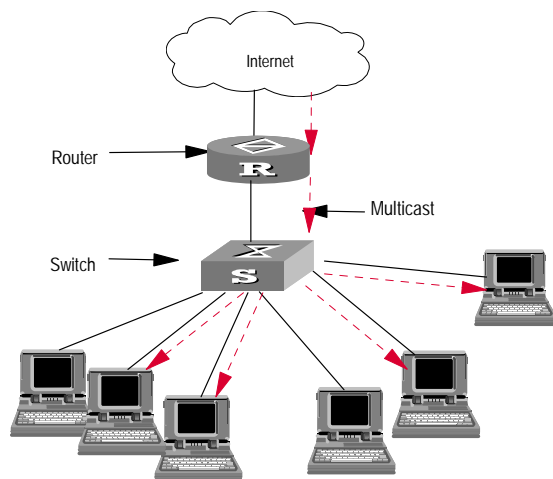


Figure 1-3 Network diagram for IGMP Snooping configuration

III. Configuration procedure

Enable IGMP Snooping in system view.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10 where no Layer 3 multicast protocol is enabled.

```
[Quidway] vlan 10
[Quidway-vlan10] igmp-snooping enable
```

1.4.2 Example 2

Configure multicast VLAN on Layer 2 and Layer 3 switches.

I. Network requirements

The following table describes the network devices involved in this example and the configurations you should make on them.

Table 1-12 Network devices and their configurations in this example

Device	Role	Description
Switch A	Layer 3 switch	The interface IP address of VLAN 20 is 168.10.1.1. The GigabitEthernet1/0/1 port is connected to the workstation and belongs to VLAN 20. VLAN 10 is the multicast VLAN. The GigabitEthernet1/0/10 port is connected to Switch B.
Switch B	Layer 2 switch	VLAN 2 contains the GigabitEthernet1/0/1 port and VLAN 3 contains the GigabitEthernet1/0/2 port. The two ports are connected to PC1 and PC2 respectively. The GigabitEthernet1/0/10 port is connected to Switch A.
PC 1	PC of User 1	PC 1 is connected to the GigabitEthernet1/0/1 port on Switch B.
PC 2	PC of User 2	PC 2 is connected to the GigabitEthernet1/0/2 port on Switch B.

Configure a multicast VLAN, so that the users in VLAN 2 and VLAN 3 can receive multicast streams through the multicast VLAN.

II. Network diagram

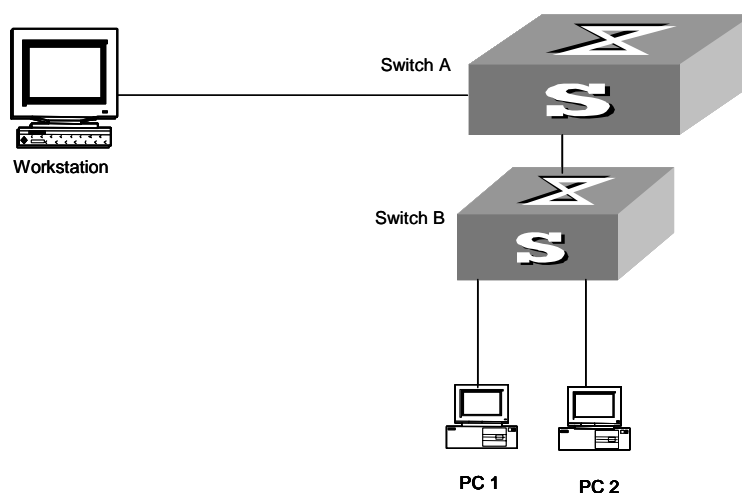


Figure 1-4 Network diagram for multicast VLAN configuration

III. Configuration procedure

The following configuration is based on the prerequisite that the devices are properly connected and all the required IP addresses are already configured.

- 1) Configure Switch A as follows:

Set the interface IP address of VLAN 20 to 168.10.1.1 and enable the PIM DM protocol on the VLAN interface.

```
<Switch A> system-view
[Switch A] multicast routing-enable
[Switch A] vlan 20
[Switch A-vlan20] interface vlan-interface 20
[Switch A-Vlan-interface20] ip address 168.10.1.1 255.255.255.0
[Switch A-Vlan-interface20] pim dm
[Switch A-Vlan-interface20] quit
```

Create VLAN 10.

```
[Switch A] vlan 10
[Switch A-vlan10] quit
```

Define the GigabitEthernet 1/0/10 port as a hybrid port, add the port to VLAN 2, VLAN 3 and VLAN 10, and make the port send VLAN 2, VLAN 3 and VLAN 10 packets with VLAN tags.

```
[Switch A] interface GigabitEthernet 1/0/10
[Switch A-GigabitEthernet 1/0/10] port link-type hybrid
[Switch A-GigabitEthernet 1/0/10] port hybrid vlan 2 3 10 tagged
[Switch A-GigabitEthernet 1/0/10] quit
```

Enable PIM DM and IGMP on VLAN 10.

```
[Switch A] multicast routing-enable
[Switch A] interface Vlan-interface 10
[Switch A-Vlan-interface10] pim dm
[Switch A-Vlan-interface10] igmp enable
```

2) Configure Switch B as follows:

Enable IGMP Snooping globally.

```
<Switch B> system-view
[Switch B] igmp-snooping enable
```

Configure VLAN 10 as a multicast VLAN and enable IGMP Snooping on it.

```
[Switch B] vlan 10
[Switch B-vlan10] service-type multicast
[Switch B-vlan10] igmp-snooping enable
[Switch B-vlan10] quit
```

Define the GigabitEthernet 1/0/10 port as a hybrid port, add the port to VLAN 2, VLAN 3 and VLAN 10, and make the port send VLAN 2, VLAN 3 and VLAN 10 packets with VLAN tags.

```
[Switch B] interface GigabitEthernet 1/0/10
[Switch B-GigabitEthernet 1/0/10] port link-type hybrid
[Switch B-GigabitEthernet 1/0/10] port hybrid vlan 2 3 10 tagged
```



```
[Switch B-GigabitEthernet 1/0/10] quit
```

Define the GigabitEthernet 1/0/1 port as a hybrid port, add the port to VLAN 2 and VLAN 10, make the port send VLAN 2 and VLAN 10 packets without VLAN tags, and set VLAN 2 as the default VLAN of the port.

```
[Switch B] interface GigabitEthernet 1/0/1
[Switch B-GigabitEthernet 1/0/1] port link-type hybrid
[Switch B-GigabitEthernet 1/0/1] port hybrid vlan 2 10 untagged
[Switch B-GigabitEthernet 1/0/1] port hybrid pvid vlan 2
[Switch B-GigabitEthernet 1/0/1] quit
```

Define the GigabitEthernet 1/0/2 port as a hybrid port, add the port to VLAN 3 and VLAN 10, make the port send VLAN 3 and VLAN 10 packets without VLAN tags, and set VLAN 3 as the default VLAN of the port.

```
[Switch B] interface GigabitEthernet 1/0/1
[Switch B-GigabitEthernet 1/0/2] port link-type hybrid
[Switch B-GigabitEthernet 1/0/2] port hybrid vlan 3 10 untagged
[Switch B-GigabitEthernet 1/0/2] port hybrid pvid vlan 3
[Switch B-GigabitEthernet 1/0/2] quit
```

1.5 Troubleshooting IGMP Snooping

Symptom: Multicast does not function on the switch.

Solution:

The reason may be:

- IGMP Snooping is not enabled. Use the **display current-configuration** command to check the status of IGMP Snooping.
- If IGMP Snooping is disabled, check whether it is disabled globally or on the corresponding VLAN. If it is disabled globally, use the **igmp-snooping enable** command in both system view and VLAN view to enable it both globally and on the corresponding VLAN. If IGMP Snooping is disabled on the VLAN, use the **igmp-snooping enable** command in VLAN view to enable it on the corresponding VLAN.
- 1) Multicast forwarding table set up by IGMP Snooping is wrong.
 - Use the **display igmp-snooping group** command to check if the multicast group is the expected one.
 - If the multicast group created by IGMP Snooping is not correct, contact your technical support personnel.
- 2) Multicast forwarding tables do not match.
 - Use the **display mac-address vlan *vlanid*** command in any view to check if the MAC multicast forwarding table established under the specified VLAN is consistent with that established by IGMP Snooping.
 - If they are not consistent, contact your technical support personnel.

Chapter 2 IGMP Group Limit on Interface

2.1 Introduction

If there is no limit on the number of IGMP groups that can be added to a multicast routing interface and the total number of IGMP groups on the switch, the switch memory may be exhausted after a number of multicast groups are added, which in turn results in trouble on the routing interface of the switch.

You can limit the number of multicast groups on a switch interface by configuring the maximum number of IGMP multicast groups on the interface. After that, when users order multicast group programs, the number of multicast groups is limited, and therefore the occupied network bandwidth is controlled. The total maximum number of IGMP groups that can be added to the routing interfaces on the switch is defined by the system and cannot be changed by any configuration command.

2.1.1 Configuring the Maximum Number of IGMP Groups on an Interface

I. Configuration preparation

You should enable the multicast function on the switch.

II. Configuration procedure

Table 2-1 Configure the maximum number of IGMP groups on an interface

Operation	Command	Description
Enter system view	system-view	—
Enable multicast routing	multicast routing-enable	Required
Enter VLAN interface view	interface vlan-interface <i>vlan-id</i>	—
Enable IGMP	igmp enable	Required
Configure the maximum number of IGMP groups that can be added to the VLAN interface	igmp group-limit <i>limit</i>	Required By default, there is no limit on the number of multicast groups that can be added to the interface.



Note:

- If the number of multicast groups that have been added to an interface reaches the limit you configured, the system will not add any new multicast group to the interface.
 - If you set the maximum number of IGMP groups on an interface to 1, the new group will take precedence over the old one. That is, when you add a new multicast group to the interface, the system automatically removes the old one from the interface and substitutes the new group for the old one.
 - If the maximum number you configured on an interface is less than the number of the existing multicast groups on the interface, the system automatically removes some earlier groups from the interface until the number of the existing multicast groups on the interface is no more than the configured number.
-

Chapter 3 Multicast MAC Address Entry Configuration

3.1 Introduction

In Layer 2 multicast, the system can add multicast forwarding entries dynamically through Layer 2 multicast protocol. However, you can also manually create a static multicast address entry to bind a port to a multicast address.

Generally, when receiving a multicast packet whose multicast address has not yet been registered on the switch, the switch broadcasts the packet in the VLAN. However, you can configure a static multicast MAC address entry to avoid this case.

3.2 Multicast MAC Address Entry Configuration

The following table describes how to configure a multicast MAC address entry.

Table 3-1 Configure a multicast MAC address entry

Operation	Command	Description
Enter system view	system-view	—
Add a multicast MAC address entry	mac-address multicast <i>mac-address interface</i> <i>interface-list vlan vlan-id</i>	Required <i>mac-address</i> must be a multicast MAC address. <i>vlan-id</i> is the VLAN ID the port belongs to.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Add a multicast MAC address entry.	mac-address multicast <i>mac-address vlan vlan-id</i>	Required This command is used in Ethernet port view. It has the same effect with the above command used in system view with the same port specified.

You can use the corresponding **undo** command to cancel the creation.



Note:

- If the multicast MAC address entry you are creating has already been existed, the system gives you a prompt.
- The switch will not learn a manually added multicast MAC address by IGMP Snooping. The **undo mac-address multicast** command can only remove manually created multicast MAC address entries and cannot remove those learned by the switch.
- When adding a port to a manually created multicast MAC address entry, you should first remove the entry, then re-create the entry and specify the port as the forward port of the entry.
- The system does not support the configuring of multicast MAC address on an IRF port. If you do this, the system will give you a prompt that the multicast MAC address configuration fails.
- You cannot enable port aggregation on a port where you have configured a multicast MAC address; and you cannot configure a multicast MAC address on an aggregated port.

3.3 Displaying Multicast MAC Address Configuration

You can use the following **display** command in any view to display the multicast MAC address entry configuration.

Table 3-2 Display multicast MAC address configuration

Operation	Command	Description
Display all the multicast MAC address entries added	display mac-address multicast static [count <i>mac-address</i> vlan <i>vlan-id</i> vlan <i>vlan-id</i>]	You can use the display command in any view.

Chapter 4 Multicast Source Deny Configuration

4.1 Introduction

The purpose of the multicast source deny feature is to filter out multicast packets on an unauthorized multicast source port to prevent the user connected to the port from setting up a multicast server without permission.

4.2 Enabling Multicast Source Deny

Table 4-1 Enable multicast source deny

Operation	Command	Description
Enter system view	system-view	—
Enable multicast source deny in system view	multicast-source-deny [interface <i>interface-list</i>]	Required <ul style="list-style-type: none"> Executing this command without specifying the <i>interface-list</i> argument will enable the feature globally (that is, on all the ports of the switch). Executing this command with the <i>interface-list</i> argument specified will enable the feature on the specified port. By default, this feature is disabled globally.
Enter Ethernet port view	interface <i>interface_type</i> <i>interface_num</i>	<i>interface_type</i> and <i>interface_num</i> are the type and number of a port.
Enable multicast source deny in Ethernet port view	multicast-source-deny	Optional By default, this feature is disabled on all the ports of the switch.

You can use the corresponding **undo** command to disable the feature.

4.3 Displaying Multicast Source Deny Configuration

You can use the following **display** command in any view to display the configuration of the multicast source deny feature.

Table 4-2 Display the configuration information about multicast source deny

Operation	Command	Description
Display the configuration information about the multicast source deny feature	display multicast-source-deny [<i>interface_type</i> interface <i>interface_number</i>]	<p>You can execute the display command in any view.</p> <ul style="list-style-type: none"> • If neither port type nor port number is specified, the command displays the multicast source deny configuration on all the ports of the switch. • If only port type is specified, the command displays the multicast source deny configuration on the specified type of ports of the switch. • If both port type and port number are specified, the command displays the multicast source deny configuration on the specified port.

Chapter 5 IGMP Snooping Configuration Commands

5.1 IGMP Snooping Configuration Commands

5.1.1 display igmp-snooping configuration

Syntax

display igmp-snooping configuration

View

Any view

Parameter

None

Description

Use the **display igmp-snooping configuration** command to display the configuration information about IGMP Snooping.

When IGMP Snooping is enabled on the switch, this command displays the following information: IGMP Snooping state, aging time of the router port, maximum query response time, and aging time of multicast member ports.

Related command: **igmp-snooping**.

Example

Display the configuration information about IGMP Snooping on the switch.

```
<Quidway> display igmp-snooping configuration
Enable IGMP-Snooping.
The router port timeout is 105 second(s).
The max response timeout is 1 second(s).
The host port timeout is 260 second(s).
```

The above information shows: IGMP Snooping has already been enabled, the aging time of the router port is 105 seconds, the maximum query response time is one second, and the aging time of multicast member ports is 260 seconds.

5.1.2 display igmp-snooping group

Syntax

display igmp-snooping group [vlan *vlan-id*]

View

Any view

Parameter

vlan *vlan-id*: Specifies a VLAN ID.

Description

Use the **display igmp-snooping group** command to display information about the IP and MAC multicast groups under one VLAN (with **vlan *vlan-id***) or all VLANs (without **vlan *vlan-id***).

This command displays the following information: VLAN ID, router port, IP multicast group address, member ports included in IP multicast group, MAC multicast group, MAC multicast group address, member ports included in MAC multicast group.

Example

Display information about the multicast groups under VLAN 2.

```
<Quidway> display igmp-snooping group vlan 2
*****Multicast group table*****
Vlan(id):2.
Router port(s):GigabitEthernet1/0/1
IP group(s):the following ip group(s) match to one mac group.
IP group address:230.45.45.1
Member port(s):GigabitEthernet1/0/2
MAC group(s):
MAC group address:01-00-5e-2d-2d-01
Member port(s):GigabitEthernet1/0/2
```

The above information shows:

- There exist multicast groups under VLAN 2.
- GigabitEthernet1/0/1 is the router port.
- The IP multicast group address is 230.45.45.1.
- GigabitEthernet1/0/2 is a member port of the IP multicast group.
- The MAC multicast group address is 0100-5e2d-2d01.
- GigabitEthernet1/0/2 is a member port of the MAC multicast group.

5.1.3 display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

Any view

Parameter

None

Description

Use the **display igmp-snooping statistics** command to display the message statistics about IGMP Snooping.

This command displays the following information: the numbers of the IGMP general query messages, IGMP group-specific query messages, IGMP V1 report messages, IGMP V2 report messages, IGMP leave messages and error IGMP messages received, and the number of the IGMP group-specific query messages sent.

Related command: **igmp-snooping**.

Example

Display the message statistics about IGMP Snooping.

```
<Quidway> display igmp-snooping statistics
Received IGMP general query packet(s) number:0.
Received IGMP specific query packet(s) number:0.
Received IGMP V1 report packet(s) number:0.
Received IGMP V2 report packet(s) number:0.
Received IGMP leave packet(s) number:0.
Received error IGMP packet(s) number:0.
Sent IGMP specific query packet(s) number:0.
```

The above information shows that IGMP Snooping has received:

- Zero IGMP general query message
- Zero IGMP group-specific query message
- Zero IGMP V1 report message
- Zero IGMP V2 report message
- Zero IGMP leave message
- Zero IGMP error message

And IGMP Snooping has sent:

- Zero IGMP group-specific query message

5.1.4 igmp-snooping

Syntax

igmp-snooping { enable | disable }

View

System view, VLAN view

Parameter

enable: Enables IGMP Snooping.

disable: Disables IGMP Snooping.

Description

Use the **igmp-snooping enable** command to enable IGMP Snooping.

Use the **igmp-snooping disable** command to disable IGMP Snooping.

By default, IGMP Snooping is disabled on the switch.

Example

Enable IGMP Snooping on the switch.

```
<Quidway>system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] igmp-snooping enable
```

5.1.5 igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave

undo igmp-snooping fast-leave

View

Ethernet port view

Parameter

None

Description

Use the **igmp-snooping fast-leave** command to enable IGMP fast leave processing.

Use the **undo igmp-snooping fast-leave** command to cancel the configuration.

By default, IGMP fast leave processing is disabled.

Normally, when receiving an IGMP Leave message, IGMP Snooping does not immediately remove the port from the multicast group, but sends a group-specific query message. If no response is received in a given period, it then removes the port from the multicast group.

If this command is executed, when receiving an IGMP Leave message, IGMP Snooping removes the port from the multicast group immediately. When the port has only one user, enabling IGMP fast leave processing can save bandwidth.

Note that, if the client(s) under the port are IGMP V2-enabled, this feature operates normally. Otherwise, when the port has multiple users, the leave of one user may disrupt the multicast to every other user under the port in the same multicast group.

Example

Enable IGMP fast leave processing on the GigabitEthernet1/0/1 port.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface GigabitEthernet 1/0/1
[Quidway-GigabitEthernet1/0/1] igmp-snooping fast-leave
```

5.1.6 igmp-snooping group-limit

Syntax

igmp-snooping group-limit [**vlan** *vlan-list* | **overflow-replace**]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View

Ethernet port view

Parameter

limit: Maximum number of multicast groups the port can join, in the range of 1 to 256.

overflow-replace: Allows new multicast groups to replace existing multicast groups in this order: the multicast group with the least IP address will be replaced first.

vlan-list: VLAN list, in the format of { *vlan-id* [**to** *vlan-id*] }&<1-10>, where *vlan-id* ranges from 1 to 4,094, and &<1-10> represents you can input at most 10 VLAN IDs/VLAN ID ranges.

Description

Use the **igmp-snooping group-limit** command to set the maximum number of multicast groups the port can join.

Use the **undo igmp-snooping group-limit** command to restore the default setting.

By default, there is no limit on the number of multicast groups the port can join.

Example

Allow the GigabitEthernet1/0/1 port to join at most 200 multicast groups.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface GigabitEthernet 1/0/1
[Quidway-GigabitEthernet1/0/1] igmp-snooping group-limit 200
```

5.1.7 igmp-snooping group-policy

Syntax

igmp-snooping group-policy *acl-number* **vlan** *vlan-list*

undo igmp-snooping group-policy **vlan** *vlan-list*

View

System view, Ethernet port view

Parameter

acl-number: Basic ACL number, in the range of 2000 to 2999.

vlan-list: VLAN list, in the format of { *vlan-id* [**to** *vlan-id*] }&<1-10>, where *vlan-id* ranges from 1 to 4,094, and &<1-10> means you can input at most 10 VLAN IDs/VLAN ID ranges.

Description

Use the **igmp-snooping group-policy** command to configure an IGMP Snooping filter ACL.

Use the **undo igmp-snooping group-policy** command to remove the IGMP Snooping filter ACL.

By default, no IGMP Snooping filter ACL is configured on the switch.

You can configure some multicast filter ACLs globally or on the switch ports connected to user ends so as to use the IGMP Snooping filter function to limit the multicast programs that the users can order. With this function, you can treat different VoD users in different ways by allowing different users to order different groups of programs.

In practice, when a user orders a multicast program, an IGMP report message is generated. When the message arrives at the switch, the switch examines the multicast filter ACL configured on the access port to determine if the port can join the corresponding multicast group or not. If yes, it adds the port to the forward port list of the multicast group. If not, it drops the IGMP report message and does not forward the corresponding data stream to the port. In this way, you can control the multicast programs that users can order.

An ACL rule defines a multicast address or a multicast address range (for example 224.0.0.1 to 239.255.255.255) and is used to:

- Allow the port(s) to join only the multicast group(s) defined in the rule by a permit statement.
- Inhibit the port(s) from joining the multicast group(s) defined in the rule by a deny statement.

Note:

- One port can belong to multiple VLANs. But for each VLAN on the port, you can configure only one ACL.
 - If no ACL rule is configured or the port does not belong to the specified VLAN, the filter ACL you configured does not take effect on the port.
 - Since most devices broadcast unknown multicast packets, this function is often used together with the unknown multicast packet drop function to prevent multicast streams from being broadcasted to a filtered port as unknown multicast.
-

Example

Configure ACL 2000 to allow users to order the multicast programs in the multicast groups of 225.0.0.0 to 225.255.255.255.

- Configure ACL 2000.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
```

- Create VLAN 2 and add the GigabitEthernet 1/0/1 port to VLAN 2.

```
[Quidway] vlan 2
[Quidway-vlan2] port GigabitEthernet 1/0/1
```

- Allow the GigabitEthernet 1/0/1 port under VLAN 2 to join only the IGMP multicast groups defined in the rule of ACL 2000.

```
[Quidway] interface GigabitEthernet 1/0/1
[Quidway-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

Configure ACL 2001 to allow users to order the multicast programs in any multicast groups except those in 225.0.0.0 to 225.0.0.255.

- Configure ACL 2001.

```
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule deny source 225.0.0.0 0.0.0.255
[Quidway-acl-basic-2001] rule permit source any
```

- Create VLAN 2 and add the GigabitEthernet 1/0/2 port to VLAN 2.

```
[Quidway] vlan 2
[Quidway-vlan2] port GigabitEthernet 1/0/2
• Allow the GigabitEthernet 1/0/2 port under VLAN 2 to join any IGMP multicast
  groups except those defined in the deny rule of ACL 2001.
[Quidway] interface GigabitEthernet 1/0/2
[Quidway-GigabitEthernet1/0/2] igmp-snooping group-policy 2001 vlan 2
```

5.1.8 igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

View

System view

Parameter

seconds: Aging time of multicast member ports, in the range of 200 to 1000 (in seconds).

Description

Use the **igmp-snooping host-aging-time** command to set the aging time of multicast member ports.

Use the **undo igmp-snooping host-aging-time** command to restore the default aging time.

By default, the aging time of multicast member ports is 260 seconds.

The aging time of multicast member ports determines the refresh frequency of multicast group members. In an environment where multicast group members change frequently, you should set a relatively short aging time, and vice versa.

Related command: **igmp-snooping**.

Example

Set the aging time of multicast member ports to 300 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping host-aging-time 300
```

5.1.9 igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

View

System view

Parameter

seconds: Maximum query response time, in the range of 1 to 25 (in seconds).

Description

Use the **igmp-snooping max-response-time** command to configure the maximum query response time.

Use the **undo igmp-snooping max-response-time** command to restore the default maximum time.

By default, the maximum query response time is 10 seconds.

The maximum response time you configured determines how long the switch can wait for a response to an IGMP Snooping query message.

Related command: **igmp-snooping** and **igmp-snooping router-aging-time**.

Example

Set the maximum response time to an IGMP Snooping query message to 15 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping max-response-time 15
```

5.1.10 igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

View

System view

Parameter

seconds: Aging time of the router port, in the range of 1 to 1000 (in seconds).

Description

Use the **igmp-snooping router-aging-time** command to configure the aging time of the router port.

Use the **undo igmp-snooping router-aging-time** command to restore the default aging time.

By default, the aging time of the router port is 260 seconds.

The router port here refers to the port connecting the Layer 2 switch to the router. The Layer 2 switch receives IGMP general query messages from the router through this port. The aging time of the router port should be a value about 2.5 times of the general query interval.

Related command: **igmp-snooping max-response-time** and **igmp-snooping**.

Example

Set the aging time of the router port to 500 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping router-aging-time 500
```

5.1.11 reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Parameter

None

Description

Use the **reset igmp-snooping statistics** command to clear the IGMP Snooping statistics.

Related command: **igmp-snooping**.

Example

```
# Clear the IGMP Snooping statistics.
<Quidway> reset igmp-snooping statistics
```

5.1.12 service-type multicast

Syntax

service-type multicast

undo service-type multicast

View

VLAN view

Parameter

None

Description

Use the **service-type multicast** command to set the current VLAN as a multicast VLAN.

Use the **undo service-type multicast** command to cancel the multicast VLAN setting.

By default, no VLAN is a multicast VLAN.

By configuring a multicast VLAN, adding corresponding switch ports to the multicast VLAN and enabling IGMP Snooping, you can make users in different VLANs share the same multicast VLAN. This saves bandwidth since multicast stream is transmitted only within the multicast VLAN, and also guarantees the security because the multicast VLAN is completely isolated from the user VLANs.

Note:

- You cannot set the isolate VLAN as a multicast VLAN.
 - One port can belong to only one multicast VLAN.
 - The port connected to a user end can only be set as a hybrid port.
 - A multicast member port must belong to the same multicast VLAN with the router port. Or else, it cannot receive multicast packets.
 - When setting a multicast VLAN ID on the router port, you must define the port as a trunk port or a tag-carried hybrid port, or else no multicast member port in this multicast VLAN can receive multicast packets.
 - If a multicast member port needs to receive multicast packets forwarded by the router port but the router port does not belong to any multicast VLAN, you should remove the multicast member port from its multicast VLAN, or else it cannot receive multicast packets.
-

Example

Configure VLAN 2 as a multicast VLAN.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] service-type multicast
```

Chapter 6 IGMP Group Limit Commands

6.1 IGMP Group Limit Commands

6.1.1 igmp group-limit

Syntax

```
igmp group-limit limit  
undo igmp group-limit
```

View

VLAN interface view

Parameter

limit: Maximum number of IGMP groups, in the range of 0 to 256.

Description

Use the **igmp group-limit** command to configure the maximum number of multicast groups that can be added to a VLAN interface. After this configuration, the Layer 3 switch does not process any new IGMP join messages if the limit is exceeded.

Use the **undo igmp group-limit** command to restore the default configuration.

By default, the maximum number of IGMP groups on a VLAN interface is 256.

Re-executing this command will overwrite the old configuration with the new one.



Note:

- If the number of multicast groups that have been added to an interface reaches the limit you configured, the system will not add any new multicast group to the interface.
 - If you set the maximum number of IGMP groups on an interface to 1, the new group will take precedence over the old one. That is, when you add a new multicast group to the interface, the system automatically removes the old one from the interface and substitutes the new group for the old one.
 - If the maximum number you configured on an interface is less than the number of the existing multicast groups on the interface, the system automatically removes some earlier groups from the interface until the number of existing multicast groups on the interface is no more than the configured number.
-

Example

Set the maximum number of IGMP groups that can be added to Vlan-interface 10 to 100.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp group-limit 100
```

Chapter 7 Multicast MAC Address Entry Configuration Commands

7.1 Multicast MAC Address Entry Configuration Commands

7.1.1 mac-address multicast interface vlan

Syntax

```
mac-address multicast mac-address interface interface-list vlan vlan-id  
undo mac-address multicast [ mac-address [ interface interface-list ] vlan vlan-id ]
```

View

System view

Parameter

mac-address: Multicast MAC address.

interface-list: Forward port list, in the format of { { *interface-type* *interface-num* | *interface-name* } [**to** { *interface-type* *interface-num* | *interface-name* }] }&<1-10>. Where, *interface-type* and *interface-num* are the type and number of a port, *interface-name* is the name of a port, and &<1-10> means you can specify up to 10 ports/port ranges. For the value ranges of the three arguments, refer to the command parameter description in the *Port Configuration* module of this document.

vlan-id: VLAN ID.

Description

Use the **mac-address multicast** command to add a multicast MAC address entry.

Use the **undo mac-address multicast** command to remove a multicast MAC address entry.

A multicast address entry contains the following information: multicast MAC address, Forward port, and VLAN ID.

Related command: **display mac-address multicast static**.

Example

```
# Add a multicast MAC address entry for VLAN 1, with the multicast MAC address  
0100-5e0a-0805 and forward port GigabitEthernet 1/0/1.
```

```
<Quidway> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] mac-address multicast 0100-5e0a-0805 interface GigabitEthernet  
1/0/1 vlan 1
```

7.1.2 mac-address multicast vlan

Syntax

```
mac-address multicast mac-address vlan vlan-id  
undo mac-address multicast [ [ mac-address ] vlan vlan-id ]
```

View

Ethernet port view

Parameter

mac-address: Multicast MAC address.

vlan-id: VLAN ID.

Description

Use the **mac-address multicast vlan** command to add a multicast MAC address entry.

Use the **undo mac-address multicast vlan** command to remove a multicast MAC address entry.

A multicast MAC address entry contains a multicast MAC address, a VLAN ID, and some other information.

Related command: **display mac-address multicast static**.

Example

Add a multicast MAC address entry for VLAN 1, with the multicast MAC address 0100-1000-1000 and forward port GigabitEthernet 1/0/1.

```
<Quidway> system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] interface GigabitEthernet1/0/1  
[Quidway-GigabitEthernet1/0/1] mac-address multicast 0100-1000-1000 vlan 1
```

7.1.3 display mac-address multicast static

Syntax

```
display mac-address multicast static [ count | mac-address vlan vlan-id | vlan  
vlan-id ]
```

View

Any view

Parameter

mac-address **vlan** *vlan-id*: Multicast MAC address entry in a specified VLAN.

count: Displays the number of the MAC address entries.

vlan-id: VLAN ID.

Description

Use the **display mac-address multicast static** command to display the multicast MAC address entries manually configured on the switch, with each entry containing the following information: multicast MAC address, VLAN ID, MAC address state, port number(s), and aging time of each port.

- Executing this command with neither *mac-address* **vlan** *vlan-id* nor **vlan** *vlan-id* will display all the multicast MAC address entries added on the switch.
- Executing this command with **vlan** *vlan-id* will display all the multicast MAC address entries added to the specified VLAN.
- Executing this command with *mac-address* **vlan** *vlan-id* will display the multicast MAC address entry added to the specified VLAN with the specified multicast MAC address.
- Executing this command with the **count** keyword will display the number of the configured multicast MAC address entries on the switch.

Example

Display all the multicast MAC address entries manually configured in VLAN 1.

```
<Quidway>display mac-address multicast static vlan 1
MAC ADDR          VLAN ID STATE          PORT INDEX          AGING TIME(s)
0100-0001-0001    1          Config static      GigabitEthernet1/0/1 N/A
                                                           GigabitEthernet1/0/2
                                                           GigabitEthernet1/0/3
                                                           GigabitEthernet1/0/4
--- 1 static mac address(es) found ---
```

Chapter 8 Multicast Source Deny Commands

8.1 Multicast Source Deny Commands

8.1.1 multicast-source-deny

Syntax

```
multicast-source-deny [ interface interface-list ]  
undo multicast-source-deny [ interface interface-list ]
```

View

System view, Ethernet port view

Parameter

interface *interface-list*: Specifies an Ethernet port list in the format of { { *interface-type* *interface-num* | *interface-name* } [**to** { *interface-type* *interface-num* | *interface-name* }] }&<1-10>. Where, *interface-type* and *interface-num* are the type and number of a port, *interface-name* is the name of a port, and &<1-10> means you can specify up to 10 ports/port ranges. For the value ranges of the three arguments, refer to the command parameter description in the *Port Configuration* module of this document.

Description

Use the **multicast-source-deny** command to enable the multicast source deny feature.

Use the **undo multicast-source-deny** command to restore the default state of the multicast source deny feature.

By default, the multicast source deny feature is disabled on every port.

The purpose of the multicast source deny feature is to filter out multicast packets on an unauthorized multicast source port to prevent the user connected to the port from setting up a multicast server without permission.

Executing this command in system view without specifying the *interface-list* argument will enable the feature globally (that is, on all the ports of the switch). Executing this command in system view with the *interface-list* argument specified will enable the feature on the specified port. Executing this command in Ethernet port view (you cannot specify the *interface-list* argument in this view) will enable the feature only on the current port.

Example

Enable multicast source deny on all ports of the switch.

```
<Quidway>system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] multicast-source-deny
```

Enable multicast source deny on the ports GigabitEthernet 1/0/1 to GigabitEthernet 1/0/10 and GigabitEthernet 1/0/12.

```
[Quidway] multicast-source-deny interface GigabitEthernet 1/0/1 to  
GigabitEthernet 1/0/10 GigabitEthernet 1/0/12
```

8.1.2 display multicast-source-deny

Syntax

display multicast-source-deny [**interface** *interface_type* *interface_number*]

View

Any view

Parameter

interface_type: Port type.

interface_number: Port number.

Description

Use the **display multicast-source-deny** command to display the configuration information about the multicast source deny feature.

Executing this command with neither port type nor port number specified will display the multicast source deny configurations on all the ports of the switch.

Executing this command with only port type specified will display the multicast source deny configurations on all the specified type of ports.

Executing this command with both port type and port number specified will display the multicast source deny configuration on the specified port.

Example

Display the state of the multicast source deny feature on the GigabitEthernet 1/0/1 port.

```
<Quidway>system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] display multicast-source-deny GigabitEthernet 1/0/1
```

Display the state of the multicast source deny feature on each 1000 Mbps Ethernet port.

```
[Quidway] display multicast-source-deny interface GigabitEthernet
```