

Multicast Configuration

1. Configuring IP Multicasting
1. Configuring IGMP Snooping

1 Configuring IP Multicasting

1.1 Overview

IP multicasting is abstracted hardware multicasting and an extended multicast routing protocol on the standard IP network layer.

In traditional IP transmission, only one host can send packets to a single host (unicast communication) or all hosts (broadcast communication). However, the multicast technology provides the third choice: a host can send packets to certain specified hosts.

IP multicasting is applicable to one-to-many multimedia applications.

1.2 Features

Overview

Feature	Description
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	Deletes the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

1.2.1 Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Working Principle

Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Related Configuration

↳ [Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries](#)

By default, the overwriting mechanism upon the overflow of multicast hardware forwarding entries is disabled.

Run **msf ipmc-overflow override** to configure the overwriting mechanism upon overflow of multicast hardware forwarding entries.

1.3 Configuration

Configuration	Description and Command
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	msf ipmc-overflow override Configures the overwriting mechanism upon overflow of multicast hardware forwarding entries.

1.3.1 Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Configuration Effect

- Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- The overwriting mechanism upon overflow of multicast hardware forwarding entries can be configured on each device unless otherwise specified.

Verification

Run **show running-config** to check whether the overwriting mechanism upon overflow of multicast hardware forwarding entries is configured.

Related Commands

↳ [Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries](#)

Command	msf ipmc-overflow override
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

↳ [Creating the IP Multicast Service on the IPv4 Network and Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries](#)

Scenario	Basic environment of the IP multicasting service (Omitted)

Configuration Steps	<ul style="list-style-type: none"> ● Configure the basic functions of IP multicasting. (Omitted) ● Configure the overwriting mechanism upon overflow of multicast hardware forwarding entries.
A	<pre>A# configure terminal A(config)#msf ipmc-overflow override</pre>
Verification	Run show running-config to check whether the overwriting mechanism upon overflow of multicast hardware forwarding entries is configured.
A	<pre>A# show running-config ... msf ipmc-overflow override ...</pre>

1.4 Monitoring

Clearing

- Running the **clear** commands may lose vital information and interrupt services.

Displaying

Description	Command
Displays the IPv4 multi-layer multicast forwarding table.	show msf msc

Debugging

Description	Command
Debugs the processing of IPv4 multi-layer multicast packet forwarding.	debug msf forwarding
Debugs the operation on multi-layer multicast forwarding entries on an IPv4 network.	debug msf msc
Debugs the bottom-layer hardware processing of IPv4 multi-layer multicast packet forwarding.	debug msf ssp
Debugs the invocation of API interfaces provided by IPv4 multi-layer multicast forwarding.	debug msf api
Debugs the processing of multi-layer multicast forwarding events on an	debug msf event

Description	Command
IPv4 network.	

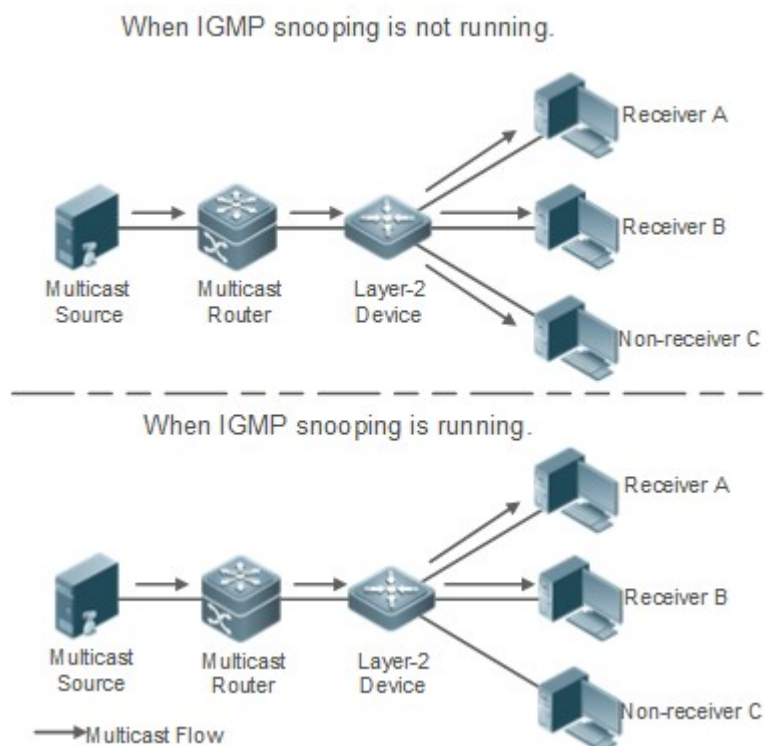
2 Configuring IGMP Snooping

2.1 Overview

Internet Group Management Protocol (IGMP) snooping is a mechanism of listening to IP multicast. It is used to manage and control the forwarding of IP multicast traffic within VLANs, realizing Layer-2 multicasting.

As shown in the following figure, when a Layer-2 device is not running IGMP snooping, IP multicast packets are broadcasted within the VLAN; when the Layer-2 device is running IGMP snooping, IP multicast packets are transmitted only to profile members.

Figure 2-1 Networking Topology of IP Multicast Forwarding within the VLAN Before and After IGMP Snooping Is Run on the Layer-2 Device



Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

2.2 Applications

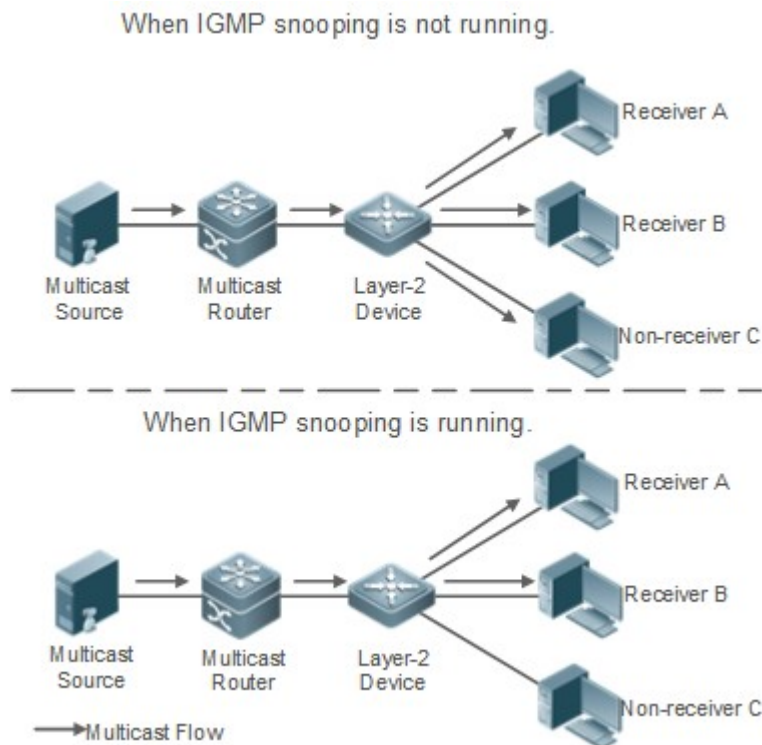
Application	Description
-------------	-------------

Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Shared Multicast Services (Multicast VLAN)	Multiple users can share the multicast traffic of the same VLAN.
Premium Channels and Preview	Controls the range of multicast addresses that allow user demanding and allows preview for profiles who are inhibited from demanding.

2.2.1 Layer-2 Multicast Control

Scenario

- As shown in the following figure, multicast packets are transmitted to users through a Layer-2 switch. When Layer-2 multicast control is not performed, namely, when IGMP snooping is not implemented, multicast packets are flooded to all the users including those who are not expected to receive these packets. After IGMP snooping is implemented, the multicast packets from an IP multicast profile will no longer be broadcast within the VLAN but transmitted to designated receivers.
- Figure 2-2 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



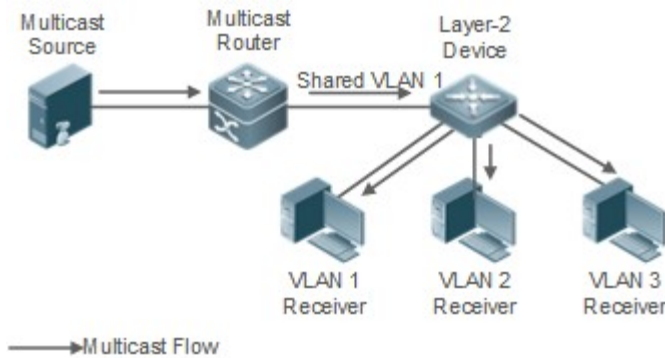
Deployment

- Configure basic IGMP snooping functions.

2.2.2 Shared Multicast Services (Multicast VLAN)

Scenario

- In Shared VLAN Group Learning (SVGL) mode or IVGL-SVGL mode (IVGL: Independent VLAN Group Learning), a device running IGMP snooping can provide shared multicast services (or multicast VLAN services) to the VLAN users. Typically, this function is used to provide the same video-on-demand (VOD) services to multiple VLAN users.
- The following figure shows the operation of a Layer-2 multicast device in SVGL mode of IGMP snooping. The multicast router sends a multicast packet to VLAN 1, and the Layer-2 multicast device automatically transfers the packet to VLAN 1, VLAN 2, and VLAN 3. In this way, the multicast services of VLAN 1 are shared by VLAN 2 and VLAN 3.
- Figure 2-3 Networking Topology of Shared Multicast Services (Multicast VLAN)



- If the Layer-2 multicast device operates in IVGL mode, the router must send a packet to each VLAN, which wastes bandwidth and burdens the Layer-2 multicast device.

Deployment

- Configure basic IGMP snooping functions (in SVGL mode or IVGL-SVG mode).

2.2.3 Premium Channels and Preview

Scenario

- In VOD application, by limiting the range of the multicast addresses that a user host can access, unpaid users will not be able to watch the premium channels. Thereafter, the preview service is offered to unpaid users before they decide whether to pay for it.
- The users can preview a premium channel for a certain period of time (for example 1 minute) after demanding it.

Deployment

- Configure basic IGMP snooping functions (in any working mode).
- Configure the range of multicast addresses that a user can access.
- Enable the preview function for VOD profiles that are denied access.

2.3 Features

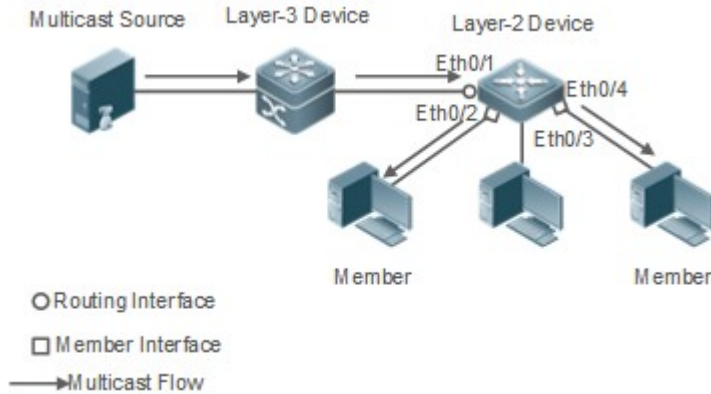
Basic Concepts

↳ Multicast Router Ports and Member Ports

- IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

The device running IGMP snooping identifies the ports within the VLAN as a multicast router port or member port so as to manage and control the forwarding of IP multicast traffic within the VLAN. As shown in the following figure, when IGMP snooping is run on a Layer-2 device, multicast traffic enters the multicast router port and exits from the member ports.

Figure 2-4 Networking Topology of Two IGMP Snooping Ports



- Multicast router port: The location of the multicast source is directed by the port on the Layer-2 multicast device which is connected to the multicast router (Layer-3 multicast device): By listening to IGMP packets, the Layer-2 multicast device can automatically detect the multicast router port and maintain the port dynamically. It also allows users to configure a static router port.
- Member port: The port is on a Layer-2 multicast device and is connected to member hosts. It directs the profile members. It is also called the Listener Port. By listening to IGMP packets, the Layer-2 multicast device can automatically detect the member port and maintain the port dynamically. It also allows users to configure a static member port.

Overview

Feature	Description
Listening to IGMP Packets	Discovers and identifies the router port and member port to establish and maintain the IGMP snooping forwarding entries. :
IGMP Snooping Working Modes	Provides independent or shared multicast services to the user VLAN.
Multicast Security Control	Controls the multicast service scope and load to prevent illegal multicast traffic.
Profile	Defines the range of multicast addresses that permit or deny user requests for reference of other functions.
Handling QinQ	Sets the forwarding mode of multicast packets on the QinQ interface.
IGMP Querier	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.

2.3.1 Listening to IGMP Packets

A device running IGMP snooping analyzes IGMP packets received, and finds and identifies the router port and member port using these packets, thereby creating and maintaining an IGMP snooping entry.

Working Principle

A device running IGMP snooping can identify and handle the following types of IGMP packets:

↳ Query Packets

- An IGMP querier periodically sends General Query packets. When the IGMP querier receives Leave packets, it sends Group-Specific Query packets.

When the device running IGMP snooping receives the Query packets, it performs the following operations within the VLAN:

- Forward the IGMP Query packets to all the ports (except the receiving port of these packets).
- If the receiving port is a dynamic router port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- If the receiving port is not a dynamic router port, use it as a dynamic router port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- For general queries, reset the aging timer for all the dynamic member ports. If the timer expires, the port will no longer be used as the dynamic member port for the general group. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- For designated query packets, reset the aging timer for all the dynamic member ports of the designated profile. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- If dynamic router port learning is disabled, IGMP snooping will not learn the dynamic router port.

↳ Report Packets

- When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a profile, it will also send a report.
- By default, IGMP Snooping is capable of processing IGMPv1 and IGMPv2 packets. For IGMPv3 Report packets, it processes profile information but does not process carried source information. IGMP Snooping v3 can be configured to process all information in IGMPv1, IGMPv2, and IGMPv3 packets.

When the device running IGMP snooping receives the Report packets, it performs the following operations within the VLAN:

- Forward the Report packets from all the router ports. After the **ip igmp snooping suppression enable** command is run in one IGMP query cycle, only the first report received by each profile will be forwarded.
- If the port on which Report packets are received is a dynamic member port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.
- If the port on which Report packets are received is not a dynamic member port, use it as a dynamic member port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.

↳ Leave Packets

- If a host requests to leave a profile, it will send a Leave packet.

When the device running IGMP snooping receives the Leave packets, it performs the following operations within the VLAN:

- Forward the leave packets from all the router ports.
- If the port on which leave packets are received is a dynamic member port and the Leave function is enabled, the port will be immediately deleted from the IGMP snooping forwarding entry of the designated profile and will no longer be used as the dynamic member port.
- If the port on which the leave packets are received is a dynamic member port and the Leave function is disabled, the port state should be maintained.

Related Configuration

↳ Configuring a Static Router Port

Run the **ip igmp snooping vlan mrouter interface** command to configure a static router port.

↳ Configuring a Static Member Port

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

↳ Enabling Report Suppression

Report suppression is disabled by default.

Run the **ip igmp snooping suppression enable** command to enable report suppression.

After report suppression is enabled, in one IGMP query cycle, only the first Report packet received by each profile will be forwarded. The source media access control (MAC) address of the forwarded report will be changed to the MAC address of the device.

↳ Enabling Immediate Leave

Immediate leave is disabled by default.

Run the **ip igmp snooping fast-leave enable** command to enable immediate leave.

↳ Enabling Dynamic Router Port Learning

Dynamic router port learning is enabled by default.

Run the **no ip igmp snooping mrouter learn pim-dvmrp** command to disable dynamic router port learning.

Run the **no ip igmp snooping vlan vid mrouter learn pim-dvmrp** command to disable dynamic router port learning for designated VLANs.

↳ Configuring the Aging Time of a Dynamic Router Port

The default aging time is 300s.

When a dynamic router port receives a query packet, the aging timer of the port is enabled or reset; if the aging time is not configured, the maximum response time carried by the query packet is used as the aging time.

Run **ip igmp snooping dyn-mr-aging-time** to configure the aging time of the dynamic router port.

↳ Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a query packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time carried by the query packet.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

↳ Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

2.3.2 IGMP Snooping Working Modes

A device running in the three modes (IVGL, SVGL, and IVGL-SVGL) of IGMP snooping can provide independent multicast services or shared multicast services to the user VLAN.

Working Principle

↳ IVGL

In IVGL mode, a device running IGMP snooping can provide independent multicast services to each user VLAN.

Independent multicast services indicate that multicast traffic can be forwarded only within the VLAN it belongs to, and a user host can subscribe to the multicast traffic within the VLAN that the host belongs to.

↳ SVGL

In SVGL mode, a device running IGMP snooping can provide shared multicast services to the user VLAN.

Shared multicast services can be provided only on shared VLANs and sub VLANs and SVGL multicast addresses are used.

In a shared VLAN, the multicast traffic within the range of SVGL multicast addresses is forwarded to a sub VLAN, and the user hosts within the sub VLAN subscribe to such multicast traffic from the shared VLAN.

- In a shared VLAN and sub VLAN, shared multicast services will be provided to the multicast traffic within the range of SVGL multicast addresses. Other multicast traffic will be discarded.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.
- When the user VLAN is set to a shared VLAN or sub VLAN, shared multicast services are provided; when a user VLAN is set to other VLANs, independent multicast services are provided.

↳ IVGL-SVGL

IVGL-SVGL mode is also called the hybrid mode. In this mode, a device running IGMP snooping can provide both shared and independent multicast services to the user VLAN.

- In a shared VLAN and sub VLAN, multicast services will be provided to the multicast traffic within an SVGL profile. For other multicast traffic, independent multicast services will be provided.
 - Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.
-
- When a user VLAN is configured as a shared VLAN or sub VLAN, both public multicast services and independent multicast services are available. When a user VLAN is configured as a VLAN other than shared VLAN and sub VLAN, only the independent multicast services are available.
-

Related Configuration

↳ **Enabling IGMP Snooping and Selecting a Working Mode**

IGMP snooping is disabled by default.

Run the **ip igmp snooping ivgl** command to enable IGMP snooping in IVGL mode.

Run the **ip igmp snooping svgl** command to enable IGMP snooping in SVGL mode.

Run the **ip igmp snooping ivgl-svgl** command to enable IGMP snooping in IVGL-SVGL mode.

A working mode must be designated when enabling IGMP snooping, namely, one of the preceding working modes must be selected.

↳ **Configuring Shared VLAN**

The shared VLAN is VLAN 1 by default.

Run the **ip igmp snooping svgl vlan** command to designate a VLAN as the shared VLAN.

In SVGL mode and IVGL-SVGL mode, only one VLAN can be configured as the shared VLAN.

↳ **Configuring Sub VLAN**

By default, a sub VLAN is any VLAN except the shared VLAN.

Run the **ip igmp snooping svgl subvlan** command to designate a VLAN as the sub VLAN.

In SVGL mode and IVGL-SVGL mode, the number of sub VLANs is not limited.

↳ **Configuring an SVGL Profile**

No default setting.

Run the **ip igmp snooping svgl profile *profile_num*** command to configure the address range of an SVGL profile.

- In SVGL mode and IVGL-SVGL mode, the SVGL profile range must be configured; otherwise, shared multicast services cannot be provided.
-

2.3.3 IGMP Security Control

A device running IGMP snooping can control the multicast service scope and load, and effectively prevents illegal multicast traffic.

Working Principle

↳ **Configuring the Profile Filtering for User Demanding**

By configuring the profile list that a user can access, you can customize the multicast service scope to guarantee the interest of operators and prevent illegal multicast traffic.

To enable this function, you should use a profile to define the range of multicast addresses that a user is allowed to access.

- When the profile is applied on a VLAN, you can define the multicast addresses that a user is allowed to access within the VLAN.
- When the profile is applied on an interface, you can define the multicast addresses that a user is allowed to access under the port.

📄 Multicast Preview

If the service provider wants to allow the users to preview some multicast video traffic that denies the users' access, and stop the multicast video traffic after the preview duration is reached, the user-based multicast preview function should be provided.

The multicast preview function is used together with multicast permission control. For example, in the application of videos, the administrator controls some premium channels by running the **ip igmp profile** command on a port or VLAN. In this way, unsubscribed users will not be able to watch these channels on demand. If users want to preview the channels before they decide whether to pay for watching or not, the multicast preview function can be enabled, allowing the premium channels to be previewed by unpaid users for a certain period of time (for example 1 minute).

📄 Controlling the Maximum Number of Profiles Allowed for Concurrent Request

If there is too much multicast traffic requested at the same time, the device will be severely burdened.

Configuring the maximum number of profiles allowed for concurrent request can guarantee the bandwidth.

- You can limit the number of profiles allowed for concurrent request globally.
- You can also limit the number of profiles allowed for concurrent request on a port.

Related Configuration

📄 Configuring the Profile Filtering

By default, profiles are not filtered and allow user access.

To filter multicast profiles, run the **ip igmp snooping filter** command in interface configuration mode or global configuration mode.

📄 Enabling Preview

Preview is not enabled by default.

Run the **ip igmp snooping preview** command to enable preview and restrict the range of the profiles permitted for multicast preview.

Run the **ip igmp snooping preview interval** to set the multicast preview duration.

📄 Configuring the Maximum Number of Profiles Allowed for Concurrent Request on a Port

By default, the number of profiles allowed for concurrent request is not limited.

Run the **ip igmp snooping max-groups** command to configure the maximum number of profiles allowed for concurrent request.

↳ Configuring the Maximum Number of Multicast Profiles Allowed Globally

By default, the maximum number of multicast profiles allowed globally is 65,536.

Run the **ip igmp snooping I2-entry-limit** command to configure the maximum number of multicast profiles allowed globally.

2.3.4 IGMP Profile

A multicast profile is used to define the range of multicast addresses that permit or deny user demanding request for reference of other functions.

Working Principle

The profile is used to define the range of multicast addresses.

When SVGL mode is enabled, an SVGL profile is used to define the range of SVGL multicast addresses.

When the multicast filter is configured on an interface, a profile is used to define the range of multicast addresses that permit or deny user request under the interface.

When a VLAN filter is configured, a profile is used to define the range of multicast addresses that permit or deny user request under within the VLAN.

When the preview function is enabled, a profile is used to define the range of multicast address allowed for preview.

Related Configuration

↳ Configuring a Profile

Default configuration:

- Create a profile, which is **deny** by default.

Configuration steps:

- Run the **ip igmp profile profile-number** command to create a profile.
- Run the **range low-address high_address** command to define the range of multicast addresses. Multiple address ranges are configured for each profile.
- (Optional) Run the **permit** or **deny** command to permit or deny user request (**deny** by default). Only one **permit** or **deny** command can be configured for each profile.

2.3.5 IGMP QinQ

Working Principle

On a device with IGMP snooping enabled and dot1q-tunnel (QinQ) port configured, IGMP snooping will handle the IGMP packets received by the QinQ port using the following two approaches:

- Approach 1: Create a multicast entry on the VLAN where IGMP packets are located. The forwarding of IGMP packets on the VLAN where these packets are located is called transparent transmission. For example, presume that IGMP

snooping is enabled for a device, Port A is designated as the QinQ port, the default VLAN of this port is VLAN 1, and it allows the passage of VLAN 1 and VLAN 10 packets. When a multicast Query packet is sent by VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 10 and forwards the multicast Query packet to the router port of VLAN 10.

- Approach 2: Create a multicast entry on the default VLAN of the QinQ port. Encapsulate the multicast packet with the VLAN tag of the default VLAN where the QinQ port is located and forward the packet within the default VLAN. For example, presume that IGMP snooping is enabled for a device, Port A is designated as the QinQ port, the default VLAN of this port is VLAN 1, and it allows the passage of VLAN 1 and VLAN 10 packets. When a multicast Query packet is sent by VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 1, encapsulates the multicast query packet with the tag of VLAN 1, and forward the packet to VLAN 1 router port.

Related Configuration

↳ Configuring QinQ

By default, IGMP snooping works in the mode specified in Approach 2.

Run the **ip igmp snooping tunnel** command to implement Approach 1.

2.3.6 IGMP Querier

On a network with a Layer-3 multicast device, the Layer-3 multicast device acts as an IGMP querier.

In this case, a Layer-2 device needs only to listen to IGMP packets to establish and maintain the forwarding entry, realizing Layer-2 multicast.

On a network without a Layer-3 multicast device, the Layer-2 multicast device must be configured with the IGMP querier function so that the device can listen to IGMP packets. In this case, a Layer-2 device needs to act as an IGMP querier as well as listen to IGMP packets to establish and maintain the forwarding entry to realize Layer-2 multicast.

Working Principle

A Layer-2 device acts as an IGMP querier to periodically send IGMP Query packets, listen to and maintain the IGMP Report packets replied by a user, and create a Layer-2 multicast forwarding entry. You can adjust relevant parameters of the Query packets sent by the IGMP querier through configuration.

When the device receives a Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP) packet, it considers that a multicast router, which will act as an IGMP querier, exists on the network and disables the querier function. In this way, IGMP routing will not be affected.

When the device receives the IGMP Query packets from other devices, it will compete with other devices for the IGMP querier.

↳ Enabling the Querier Function

You can enable the querier for a specific VLAN or all VLANs.

Only when the global querier function is enabled can the queriers for specific VLANs take effect.

↳ Specifying the IGMP Version for a Querier

The version of IGMP used for sending Query packets can be configured as IGMPv1, IGMPv2, or IGMPv3.

↳ [Configuring the Source IP Address of a Querier](#)

You can configure the source IP address of a query packet sent by the querier based on VLANs.

When the source IP address of the querier is not configured, the querier will not take effect.

↳ [Configuring the Query Interval of a Querier](#)

You can configure the intervals for sending global Query packets based on different queriers on different VLANs.

↳ [Configuring the Maximum Response Time of a Query Packet](#)

You can configure the maximum response time carried by a Query packet that is sent by a querier. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1. You can configure different maximum response time for queriers on different VLANs.

↳ [Configuring the Aging Time of a Querier](#)

When other IGMP queriers exist on a network, the existing device will compete with other queriers. If the existing device fails to be elected and is in the non-querier state, the aging timer of a querier will be enabled. After the timer expires, other queriers on the network are considered as expired and the existing device will be resumed as the querier.

Related Configuration

↳ [Enabling the Querier Function](#)

By default, the querier function of a device is disabled.

Run the **ip igmp snooping querier** command to enable the global querier function.

Run the **ip igmp snooping vlan num querier** command to enable the querier function for specific VLANs.

↳ [Specifying the IGMP Version for a Querier](#)

By default, a querier runs IGMPv2.

Run the **ip igmp snooping querier version** command to configure the global querier version.

Run the **ip igmp snooping vlan querier version** command to specify the querier version for specific VLANs.

↳ [Configuring the Source IP Address of a Querier](#)

By default, the source IP address of a querier is 0.

Run the **ip igmp snooping querier address** command to enable global source IP addresses of queriers.

Run the **ip igmp snooping vlan querier address** command to specify the source IP addresses of the queriers on specific VLANs.

↳ [Configuring the Query Interval of a Querier](#)

By default, the query interval of a querier is 60s.

Run the **ip igmp snooping querier query-interval** command to enable the global query interval of queriers.

Run **ip igmp snooping vlan querier query-interval** to specify the global query interval of the queriers on specific VLANs.

↳ Configuring the Maximum Response Time of a Query Packet

By default, the maximum response time of a query packet is 10s.

Run the **ip igmp snooping querier max-response-time** command to configure the maximum response time of the query packets sent by global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to specify the maximum response time of the query packets sent by the queriers on specific VLANs.

↳ Configuring the Aging Time of a Querier

By default, the aging time of a querier is 125s.

Run the **ip igmp snooping querier max-response-time** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to configure the aging time of queriers on specific VLANs.

2.4 Configuration

Configuration	Description and Command									
Configuring Basic IGMP Snooping Functions (IVGL Mode)	<ul style="list-style-type: none"> Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL mode. 									
	<table border="1"> <tr> <td>ip igmp snooping ivgl</td> <td>Enables global IGMP snooping in IVGL mode.</td> </tr> <tr> <td>no ip igmp snooping vlan <i>num</i></td> <td>Disables IGMP snooping for a VLAN.</td> </tr> </table>	ip igmp snooping ivgl	Enables global IGMP snooping in IVGL mode.	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.					
	ip igmp snooping ivgl	Enables global IGMP snooping in IVGL mode.								
no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.									
<table border="1"> <tr> <td>ip igmp snooping svgl</td> <td>Enables global IGMP snooping in SVGL mode.</td> </tr> <tr> <td>no ip igmp snooping vlan <i>num</i></td> <td>Disables IGMP snooping for a VLAN.</td> </tr> <tr> <td>ip igmp snooping svgl profile <i>profile_num</i></td> <td>Configures the SVGL profile.</td> </tr> <tr> <td>ip igmp snooping svgl vlan</td> <td>Specifies the SVGL shared VLAN.</td> </tr> <tr> <td>ip igmp snooping svgl subvlan</td> <td>Specifies the SVGL sub VLAN.</td> </tr> </table>	ip igmp snooping svgl	Enables global IGMP snooping in SVGL mode.	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.	ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.
ip igmp snooping svgl	Enables global IGMP snooping in SVGL mode.									
no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.									
ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.									
ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.									
ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.									
Configuring Basic IGMP Snooping Functions (IVGL-SVGL Mode)	<ul style="list-style-type: none"> Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL-SVGL mode. 									
	<table border="1"> <tr> <td>ip igmp snooping ivgl-svgl</td> <td>Enables global IGMP snooping in IVGL-SVGL mode.</td> </tr> <tr> <td>no ip igmp snooping vlan <i>num</i></td> <td>Disables IGMP snooping for a VLAN.</td> </tr> <tr> <td>ip igmp snooping svgl profile <i>profile_num</i></td> <td>Configures the SVGL profile.</td> </tr> <tr> <td>ip igmp snooping svgl vlan</td> <td>Specifies the SVGL shared VLAN.</td> </tr> </table>	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.	
	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.								
	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.								
	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.								
ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.									
<table border="1"> <tr> <td>ip igmp snooping ivgl-svgl</td> <td>Enables global IGMP snooping in IVGL-SVGL mode.</td> </tr> <tr> <td>no ip igmp snooping vlan <i>num</i></td> <td>Disables IGMP snooping for a VLAN.</td> </tr> <tr> <td>ip igmp snooping svgl profile <i>profile_num</i></td> <td>Configures the SVGL profile.</td> </tr> <tr> <td>ip igmp snooping svgl vlan</td> <td>Specifies the SVGL shared VLAN.</td> </tr> </table>	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.		
ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.									
no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.									
ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.									
ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.									
<table border="1"> <tr> <td>ip igmp snooping ivgl-svgl</td> <td>Enables global IGMP snooping in IVGL-SVGL mode.</td> </tr> <tr> <td>no ip igmp snooping vlan <i>num</i></td> <td>Disables IGMP snooping for a VLAN.</td> </tr> <tr> <td>ip igmp snooping svgl profile <i>profile_num</i></td> <td>Configures the SVGL profile.</td> </tr> <tr> <td>ip igmp snooping svgl vlan</td> <td>Specifies the SVGL shared VLAN.</td> </tr> </table>	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.		
ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.									
no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.									
ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.									
ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.									
<table border="1"> <tr> <td>ip igmp snooping ivgl-svgl</td> <td>Enables global IGMP snooping in IVGL-SVGL mode.</td> </tr> <tr> <td>no ip igmp snooping vlan <i>num</i></td> <td>Disables IGMP snooping for a VLAN.</td> </tr> <tr> <td>ip igmp snooping svgl profile <i>profile_num</i></td> <td>Configures the SVGL profile.</td> </tr> <tr> <td>ip igmp snooping svgl vlan</td> <td>Specifies the SVGL shared VLAN.</td> </tr> </table>	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.		
ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.									
no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.									
ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.									
ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.									

	ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.
Configuring the Packet Processing	<ul style="list-style-type: none"> (Optional) It is used to adjust relevant configurations for processing protocol packets. 	
	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	Configures a static router port.
	p igmp snooping vlan <i>vid</i> static group-address interface <i>interface-type</i> <i>interface-number</i>	Configures a static member port.
	ip igmp snooping vlan <i>vlan-id</i> mrouter learn pim-dvmrp	Enables dynamic router port learning.
	ip igmp snooping dyn-mr-aging-time <i>time</i>	Configures the aging time of a dynamic router port.
	ip igmp snooping host-aging-time <i>time</i>	Configures the aging time of a dynamic member port.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	ip igmp snooping port-fast-leave enable	Configures fast-leave in a port
	ip igmp snooping query-max-response-time <i>time</i>	Configures the maximum response time of an IGMP query packet.
	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.
	ip igmp snooping suppression svgl vlan enable	Enables IGMP Report packet suppression on SVGL shared VLAN.
	ip igmp snooping suppression vlan <i>vlan-id</i> sip <i>address</i>	Configures source IP in IGMP Report packet
Configuring IGMP Security Control	<ul style="list-style-type: none"> (Optional) It used to guarantee the security when a user requests a multicast profile. 	
	ip igmp snooping filter <i>profile-number</i>	Configures the profile filtering for user access.
	ip igmp snooping vlan <i>num</i> filter <i>profile-number</i>	Configures the per-VLAN profile filtering for user access.
	ip igmp snooping l2-entry-limit <i>number</i>	Configures the maximum number of profiles globally for user access.
	ip igmp snooping max-groups <i>number</i>	Configures the maximum number of dynamic profiles for user access.
	ip igmp snooping preview <i>profile-number</i>	Enables the preview function for a specified profile.
	ip igmp snooping preview interval <i>num</i>	Configures the preview duration.
Configuring an IGMP Profile	<ul style="list-style-type: none"> (Optional) It is used to define the range of multicast addresses that permits or denies the access of a user host. 	
	ip igmp profile <i>profile-number</i>	Creates a profile.

	range <i>low-address high_address</i>	Configures the profile range.
	permit	Permits the access of a user host.
	deny	Denies the access of a user host.
Configuring IGMP QinQ	<ul style="list-style-type: none"> (Optional) It is used to configure QinQ interface to forward multicast packets using the VLAN identifier (VID) carried by packets. 	
	ip igmp snooping tunnel	Configures QinQ to transmit IGMP packets transparently.
Configuring an IGMP Querier	<ul style="list-style-type: none"> (Optional) It is used to enable IGMP querier function on a network without a Layer-3 multicast device. 	
	ip igmp snooping querier	Enables global querier function.
	ip igmp snooping vlan num querier	Enables the querier for a VLAN.
	ip igmp snooping querier version num	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan num querier version num	Specifies the IGMP version for a querier of a VLAN.
	ip igmp snooping querier address a.b.c.d	Configures the source IP address of queriers globally.
	ip igmp snooping vlan num querier address a.b.c.d	Configures the source IP address for a querier of a VLAN.
	ip igmp snooping querier query-interval num	Configures the query interval of queriers globally.
	ip igmp snooping vlan num querier query-interval num	Configures the query interval for a querier of a VLAN.
	ip igmp snooping querier max-response-time num	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan num querier max-response-time num	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry num	Configures the aging timer for queriers globally.
ip igmp snooping vlan num querier timer expiry num	Configures the aging timer for a querier of a VLAN.	

2.4.1 Configuring Basic IGMP Snooping Functions (IVGL Mode)

Configuration Effect

- Enable IGMP snooping to realize Layer-2 multicast.
- Provide independent multicast services to each VLAN.

Notes

- IP multicast cannot be realized in SVGL mode. If IP multicast must be used, select the IVGL mode.

Configuration Steps

↳ Enabling Global IGMP Snooping in IVGL Mode

Mandatory.

After IGMP snooping is enabled globally, this function will be enabled for all VLANs.

If not specified, it is advised to run global IGMP snooping on all the devices connected user hosts.

↳ Disabling IGMP Snooping for a VLAN

(Optional) You can use this function if you wish to disable IGMP snooping on specified VLANs.

Only when global IGMP snooping is enabled can it be disabled on specified VLANs.

In IVGL mode, each VLAN can enjoy independent multicast services. Disabling any VLAN multicast services will not interfere in the services provided to the others.

Verification

- Run the **show ip igmp snooping gda-table** command to display the IGMP snooping forwarding table and verify that the member ports include only those connecting member hosts.
- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL mode.

Related Commands

↳ Enabling Global IGMP Snooping in IVGL Mode

Command	ip igmp snooping ivgl
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on all VLANs. By default, IGMP snooping is disabled.

↳ Disabling IGMP Snooping for a VLAN

Command	no ip igmp snooping vlan <i>num</i>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Only when global IGMP snooping is enabled can it be disabled on specified VLANs. In IVGL mode, you can disable IGMP snooping on any VLAN.

↳ Displaying the IGMP Snooping Entry

Command	show ip igmp snooping gda-table
----------------	--

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

↳ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL mode, the following information is displayed: <pre>IGMP Snooping running mode: IVGL</pre>

Configuration Example

↳ Providing Layer-2 Multicast Services for the Subnet Hosts

Scenario Figure 2-5	<p>The diagram illustrates a network topology for multicast services. A source host (10.1.1.1/24) is connected to Device A (a multicast router) through interface Gi 0/1. Device A has an IP address of 192.168.1.1 in VLAN 1 and is also connected to Device B (a Layer-2 device) through interface Gi 0/2. Device B is connected to three receiver hosts (Receiver 1, Receiver 2, and Receiver 3) through interfaces Fa 0/2, Fa 0/3, and Fa 0/4 respectively. All devices are part of VLAN 1, which is also associated with the 10.1.1.2/24 subnet.</p>
	<p>A is the multicast router and is connected directly to the multicast source.</p> <p>B is the Layer-2 device and is connected directly to the user host.</p> <p>Receiver 1, Receiver 2, and Receiver 3 belong to VLAN 1.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode.
A	<pre>A# configure terminal A(config)# ip multicast-routing</pre>

	<pre>A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
B	<pre>B# configure terminal B(config)# ip igmp snooping ivgl</pre>
Verification	<p>Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G.</p> <ul style="list-style-type: none"> ● Confirm that the packets (10.1.1.1 and 229.1.1.1) are received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the port (10.1.1.1, 229.1.1.1, 1) includes only Fa0/2. ● Check whether the IGMP snooping working mode is IVGL.
B	<pre>B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(1) 2 OPORTS: FastEthernet 0/1(M) FastEthernet 0/2(D)</pre> <pre>B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable</pre>

```
IGMP Preview group aging time : 60(Seconds)
```

```
Dynamic Mroute Aging Time : 300(Seconds)
```

```
Dynamic Host Aging Time : 260(Seconds)
```

```
vlan 1
```

```
-----  
IGMP Snooping state: Enable
```

```
Multicast router learning mode: pim-dvmrp
```

```
IGMP Fast-Leave: Disabled
```

```
IGMP VLAN querier: Disable
```

```
IGMP VLAN Mode: STATIC
```

Common Errors

- The working mode of IGMP snooping is improper.

2.4.2 Configuring Basic IGMP Snooping Functions (SVGL Mode)

Configuration Effect

- Enable IGMP snooping and select SVGL mode to realize Layer-2 multicast.
- Share the VLAN multicast services.

Configuration Steps

↳ Enabling Global IGMP Snooping in SVGL Mode

Mandatory.

Enable global IGMP snooping in SVGL mode.

Configure the range of associated SVGL profiles.

↳ Specifying the SVGL Shared VLAN

(Optional) By default, VLAN 1 is used as the shared VLAN. You can adjust this configuration for other options.

↳ Specifying the SVGL Sub VLAN

(Optional) By default, all the VLANs are used as the sub VLANs of SVGL and can share the multicast services of the shared VLAN. You can adjust this configuration for other options.

Verification

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in SVGL mode.

- Run the **show ip igmp snooping gda-table** command to check whether inter-VLAN multicast entries are properly formed.

Related Commands

↳ Enabling Global IGMP Snooping in SVGL Mode

Command	ip igmp snooping svgl
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the SVGL mode is selected, the range of profiles within SVGL multicast addresses needs to be associated.

↳ Configuring the SVGL profile

Command	ip igmp snooping svgl profile <i>profile_num</i>
Parameter Description	<i>profile_num</i> : Configures SVGL to associate a profile.
Command Mode	Global configuration mode
Usage Guide	By default, no profile is associated with SVGL.

↳ Specifying the SVGL Shared VLAN

Command	ip igmp snooping svgl vlan <i>vid</i>
Parameter Description	<i>vid</i> : Indicates a VLAN.
Command Mode	Interface configuration mode
Usage Guide	By default, VLAN 1 is used as the shared VLAN.

↳ Specifying the SVGL Sub VLAN

Command	ip igmp snooping svgl subvlan <i>vid-range</i>
Parameter Description	<i>vid-range</i> : Indicates VLAN ID or the range of VLAN IDs.
Command Mode	Interface configuration mode
Usage Guide	By default, all the VLANs except the shared VLAN are used as sub VLANs.

↳ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
Parameter	N/A

Description	
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in SVGL mode, the following information is displayed: <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;">IGMP Snooping running mode: SVGL</div>

Configuration Example

↳ Enabling SVGL on the Access Device

<p>Scenario Figure 2-6</p>	
	<p>A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1 is connected to VLAN 2, Receiver 2 is connected to VLAN 3, and Receiver 3 is connected to VLAN 4.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select SVGL mode. ● Configure the range of associated SVGL multicast addresses on B.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
<p>B</p>	<pre>B# configure terminal</pre>

	<pre>B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping svgl B(config)#ip igmp snooping svgl profile 1</pre>
Verification	<p>Send packets from the source (10.1.1.1) to G (229.1.1.1) and add Receiver 1, Receiver 2 and Receiver 3 to G.</p> <ul style="list-style-type: none"> ● Confirm that the packets (10.1.1.1 and 224.1.1.1) are received by Receiver 1, Receiver 2, and Receiver 3. ● Display the IGMP snooping forwarding entry on B and ensure that the ports (*, 224.1.1.1, 1) include Gi0/2, Gi0/3, and Gi0/4. ● Check whether the IGMP snooping working mode is SVGL.
B	<pre>B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D) B# show ip igmp snooping IGMP Snooping running mode: SVGL IGMP Snooping L2-entry-limit: 65536 SVGL vlan: 1 SVGL profile number: 1 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable</pre>

```
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

Common Errors

- The SVGL profile is not configured.
- The sent multicast traffic is not within the SVGL profile.

2.4.3 Configuring Basic IGMP Snooping Functions (IVGL-SVGL Mode)

Configuration Effect

- Enable IGMP snooping and select IVGL-SVGL mode to realize Layer-2 multicast.
- The SVGL profiles can share the multicast services.
- The non-SVGL profiles run in IVGL mode.

Configuration Steps

↳ Enabling Global IGMP Snooping in IVGL-SVGL Mode

Mandatory.

Enable global IGMP snooping in IVGL-SVGL mode.

Configure the range of associated SVGL profiles.

↳ Specifying the SVGL Shared VLAN

(Optional) By default, VLAN 1 is used as the shared VLAN. You can adjust this configuration for other options.

↳ Specifying the SVGL Sub VLAN

(Optional) By default, all the VLANs are used as the sub VLANs of SVGL and can share the multicast services of the shared VLAN. You can adjust this configuration for other options.

Verification

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL-SVGL mode.
- Run the **show ip igmp snooping gda-table** command to check whether inter-VLAN multicast entries are properly formed for the SVGL profiles.

- Run the **show ip igmp snooping gda-table** command to check whether intra-VLAN multicast entries are properly formed for the SVGL profiles.

Related Commands

↳ Enabling Global IGMP Snooping in IVGL-SVGL Mode

Command	ip igmp snooping ivgl-svgl
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the IVGL-SVGL mode is selected, the SVGL profiles needs to be associated.

↳ Configuring the SVGL Profile

Command	ip igmp snooping svgl profile <i>profile_num</i>
Parameter Description	<i>profile_num</i> : Configures SVGL to associate a profile.
Command Mode	Global configuration mode
Usage Guide	By default, no profile is associated with SVGL.

↳ Specifying the SVGL Shared VLAN

Command	ip igmp snooping svgl vlan <i>vid</i>
Parameter Description	<i>vid</i> : Indicates a VLAN.
Command Mode	Interface configuration mode
Usage Guide	By default, VLAN 1 is used as the shared VLAN.

↳ Specifying the SVGL Sub VLAN

Command	ip igmp snooping svgl subvlan <i>vid-range</i>
Parameter Description	<i>vid-range</i> : Indicates VLAN ID or the range of VLAN IDs.
Command Mode	Interface configuration mode
Usage Guide	By default, all the VLANs except the shared VLAN are used as sub VLANs.

↳ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
Parameter Description	N/A

Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in SVGL mode, the following information is displayed: <div style="background-color: #f0f0f0; padding: 2px;">IGMP Snooping running mode: SVGL</div>

↘ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL-SVGL mode, the following information is displayed: <div style="background-color: #f0f0f0; padding: 2px;">IGMP Snooping running mode: IVGL-SVGL</div>

Configuration Example

↘ Enabling IVGL-SVGL on the Access Device

Scenario Figure 2-7	
	<p>A is the multicast router and is connected directly to multicast Source 1.</p> <p>B is a Layer-2 device and is connected directly to the user host and multicast Source 2.</p> <p>Receiver 1 is connected to VLAN 2, Receiver 2 is connected to VLAN 3, and Receiver 3 is connected to VLAN 4.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL-SVGL mode. ● Configure the range of associated SVGL multicast addresses on B.

A	<pre> A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit </pre>
B	<pre> B# configure terminal B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping ivgl-svgl B(config)#ip igmp snooping svgl profile 1 </pre>
Verification	<p>Send packets from Source 1 (10.1.1.1) to G (224.1.1.1) and add Receiver 1, Receiver 2 and Receiver 3 to G.</p> <p>Send packets from Source 2 (192.168.2.1) to the destination (239.1.1.1) and add Receiver 1 239.1.1.1.</p> <ul style="list-style-type: none"> ● Confirm that the packets (10.1.1.1 and 224.1.1.1) are received by Receiver 1, Receiver 2, and Receiver 3. ● Check that packets (192.168.2.1 and 239.1.1.1) can be received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the ports (*, 224.1.1.1, 1) include Gi0/2, Gi0/3, and Gi0/4, and the port (*, 239.1.1.1, 1) is Gi0/2. ● Check whether the IGMP snooping working mode is IVGL-SVGL.
B	<pre> B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) </pre>

```
VLAN(4) 1 OPORTS:  
  GigabitEthernet 0/4(D)  
(*239.1.1.1, 2):  
VLAN(2) 1 OPORTS:  
GigabitEthernet 0/2(D)
```

```
B# show ip igmp snooping  
IGMP Snooping running mode: IVGL-SVGL  
IGMP Snooping L2-entry-limit: 65536  
SVGL vlan: 1  
SVGL profile number: 0  
Source port check: Disable  
Source ip check: Disable  
IGMP Fast-Leave: Disable  
IGMP Report suppress: Disable  
IGMP Globle Querier: Disable  
IGMP Preview: Disable  
IGMP Tunnel: Disable  
IGMP Preview group aging time : 60(Seconds)  
Dynamic Mroute Aging Time : 300(Seconds)  
Dynamic Host Aging Time : 260(Seconds)
```

Common Errors

- The SVGL profile is not configured.
- The sent multicast traffic is not within the SVGL profile.
- The IVGL multicast traffic cannot be forwarded within the SVGL profile.

2.4.4 Configuring the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all profiles.
- Configure specified ports as the static member ports to receive the multicast traffic from specified profiles
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or profile to the router port within a query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network.
- Configure the immediate-leave function to delete a port from the entry of member ports when a leave packet is received by the port.
- Disable dynamic router port learning to disable the learning of any router port.
- Based on network load and configuration of a multicast device, you can adjust the aging time of a router port and member port as well as the maximum response time of a query packet.

Notes

- Only when basic IGMP snooping is configured can relevant configurations take effect.

Configuration Steps

↘ **Configuring a Static Router Port**

- Optional.
- You can perform this configuration if you want to specify a static port to receive all the multicast traffic within the VLAN.

↘ **Configuring a Static Member Port**

- Optional.
- You can perform this configuration if you want to specify a static port to receive specific multicast traffic within the VLAN.

↘ **Enabling Report Packet Suppression**

- Optional.
- When there are numerous receivers to receive the packets from the same multicast profile, you can enable Report packets suppression to suppress the number of Report packets to be sent.

↘ **Enabling the Immediate-Leave Function**

- Optional.
- When there is only one receiver on a port, you can enable Leave to speed up the convergence of protocol upon leave.

↘ **Disabling Dynamic Router Port Learning**

- Optional.
- This function is used when multicast traffic needs to be forwarded only within the Layer-2 topology but not to a Layer-3 router.

↘ **Configuring the Aging Time of a Dynamic Router Port**

- Optional.
- You can configure the aging time based on network load.

↘ **Configuring the Aging Time of a Dynamic Member Port**

- Optional.
- You can configure the aging time based on the interval for sending IGMP query packets by the connected multicast router. Typically, the aging time is calculated as follows: Interval for sending IGMP query packets x 2 + Maximum response time of IGMP packets

↘ **Configuring the Maximum Response Time of a Query Packet**

- Optional.
- You can configure the aging time based on network load.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

↘ **Configuring a Static Router Port**

Command	ip igmp snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i>
Parameter	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094.
Description	<i>interface-type interface-number</i> : Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	<p>In SVGL mode, if a sub VLAN is not configured, only the configurations for the static router port within the shared VLAN can take effect, and the others can be configured but cannot take effect. If a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect.</p> <p>In IVGL-SVGL mode, if a sub VLAN is not configured, the configurations for the static router ports within all the VLANs can take effect; if a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect.</p> <p>In IVGL mode, the configurations for the static router ports within all the VLANs can take effect.</p>

↘ **Configuring a Static Member Port**

Command	ip igmp snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type</i> <i>interface-number</i>
Parameter Description	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094. <i>group-address</i> : Indicates a profile address. <i>interface-type interface-number</i> : Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

↳ Enabling Report Packet Suppression

Command	ip igmp snooping suppression enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, and the IGMPv3 Report packets cannot be suppressed.

↳ Enabling Report Packet Suppression on SVGL

Command	ip igmp snooping suppression svgl vlan enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression svgl vlan is enabled, only the first Report packet from shared VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, and the IGMPv3 Report packets cannot be suppressed.

↳ Configures Source IP in IGMP Report packet

Command	ip igmp snooping suppression vlan <i>vlan-id</i> sip <i>address</i>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, the device can customize the source IP address of a report packet globally or based on a VLAN. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, and the IGMPv3 Report packets cannot be suppressed.

↳ Enabling the Immediate-Leave Function

Command	ip igmp snooping fast-leave enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address.</p> <p>The immediate-leave function applies only to the scenario where only one host is connected to a device port. It is used to conserve bandwidth and resources.</p>

↳ Enabling the Immediate-Leave Function on port

Command	ip igmp snooping port-fast-leave enable
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	<p>When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address.</p> <p>The immediate-leave function applies only to the scenario where only one host is connected to a device port. It is used to conserve bandwidth and resources.</p>

↳ Enabling Dynamic Router Port Learning

Command	ip igmp snooping [vlan <i>vid</i>] mrouter learn pim-dvmrp
Parameter Description	vlan <i>vid</i> : Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	<p>A router port is the port that is connected directly to a multicast device running IGMP snooping and a multicast neighbor device running multicast routing protocol. By default, dynamic router port learning is enabled and the device automatically listens to IGMP Query packets, DVMRP packets, and PIM Hello packets.</p>

↳ Configuring the Aging Time of a Dynamic Router Port

Command	ip igmp snooping dyn-mr-aging-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the aging time of a dynamic router port in the unit of seconds. The value ranges from 1 to 3,600.

Command Mode	Global configuration mode
Usage Guide	<p>If a dynamic router port does not receive an IGMP general query packet or a PIM Hello packet before the aging timer expires, the device will delete this port from the router port entry.</p> <p>When dynamic router port learning is enabled, you can run this command to adjust the aging time of the dynamic router port. If the aging time is too short, the multicast device may frequently add or delete a router port.</p>

↘ Configuring the Aging Time of a Dynamic Member Port

Command	ip igmp snooping host-aging-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	<p>The aging time of a dynamic member port indicates the time when a device port receives the IGMP join packet sent from host for subscribing to an IP multicast profile.</p> <p>When the IGMP join packet is received, the aging time of the dynamic member port will be reset. The value of the timer time is host-aging-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. After the aging time is configured, the aging time of following received IGMP join packets will be host-aging-time. This configuration takes effect after the next IGMP join packet is received, and the timer of the port in use will not be refreshed.</p>

↘ Configuring the Maximum Response Time of a Query Packet

Command	ip igmp snooping query-max-response-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the maximum response time.
Command Mode	Global configuration mode
Usage Guide	<p>When an IGMP general Query packet is received, the multicast device will reset the aging time of all the dynamic member ports, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port.</p> <p>When an IGMP profile-specific Query packet is received, the multicast device will reset the aging time of all the dynamic member ports of the specific profile, which is query-max-response-time.</p> <p>If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port.</p> <p>This configuration takes effect after the next Query packet is received, and the timer in use will not be refreshed. The timer of an IGMPv3 profile-specific Query packet is not refreshed.</p>

↘ Displaying Router Ports

Command	show ip igmp snooping mroute
----------------	-------------------------------------

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the router port is successfully configured, an "S" will be displayed in the port information.</p> <pre>Orion Alpha A28X(config)#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)</pre>

↘ Displaying the Information of Dynamic Router Port Learning

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>Run the show ip igmp snooping command to display the aging time and learning status of the dynamic router port.</p> <pre>Dynamic Mroute Aging Time : 300(Seconds) Multicast router learning mode: pim-dvmrp</pre>

↘ Displaying the Information of a Member Port

Command	show ip igmp snooping gda-table
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the member port is successfully configured, an "S" will be displayed in the port information.</p> <pre>Orion Alpha A28X(config)#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1):</pre>

	VLAN(1) 1 OPORTS: GigabitEthernet 0/1(S)
--	---

↘ Displaying Other Parameters

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>Run the show ip igmp snooping command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave.</p> <pre> IGMP Fast-Leave: Enable IGMP Report suppress: Enable Query Max Response Time: 20(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds) </pre>

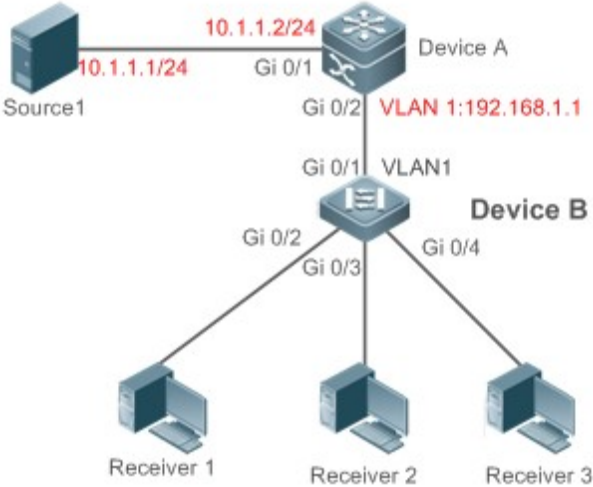
Configuration Example

↘ Configuring a Static Router Port and Static Member Port

Configuration Steps	<ul style="list-style-type: none"> ● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
	<pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Orion Alpha A28X(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Orion Alpha A28X(config)# end </pre>
Verification	Run the show ip igmp snooping mrouter and show ip igmp snooping gda-table commands to check whether the configuration takes effect.
	<pre> Orion Alpha A28X#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/0(S) </pre>

Configuration Steps	<ul style="list-style-type: none"> ● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
	<pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Orion Alpha A28X(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Orion Alpha A28X(config)# end </pre>
Verification	Run the show ip igmp snooping mrouter and show ip igmp snooping gda-table commands to check whether the configuration takes effect.
	<pre> Orion Alpha A28X#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/0(SM) </pre>

↳ Enabling Report Packet Suppression

Scenario Figure 2-8	
	<p>A is the multicast router and is connected directly to multicast Source 1.</p> <p>B is a Layer-2 device and is connected directly to the user host and multicast Source 2.</p> <p>Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1

	<p>and VLAN 1).</p> <ul style="list-style-type: none"> ● Enable IGMP snooping on B and select IVGL mode. ● Enable Report packets suppression on B.
A	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
B	<pre>B# configure terminal B(config)# ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable</pre>
Verification	<p>Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.</p>
B	<pre>B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)</pre>

↘ **Configuring Other Parameters**

Configuration Steps	<ul style="list-style-type: none"> ● Configure basic IGMP snooping functions. ● Enable Immediate-leave function.
----------------------------	--

	<ul style="list-style-type: none"> ● Disable router port learning. ● Configure the aging time of a router port. ● Configuring the aging time of a member port. ● Configure the response time of a Query packet.
	<pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip igmp snooping fast-leave enable Orion Alpha A28X(config)# no ip igmp snooping mrouter learn pim-dvmrp Orion Alpha A28X(config)#ip igmp snooping dyn-mr-aging-time 200 Orion Alpha A28X(config)#ip igmp snooping host-aging-time 100 Orion Alpha A28X(config)#ip igmp snooping query-max-response-time 60 Orion Alpha A28X(config)# end </pre>
Verification	Run the show ip igmp snooping command to check whether the configuration is successful.
	<pre> Orion Alpha A28X#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 200(Seconds) Dynamic Host Aging Time : 100(Seconds) </pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

2.4.5 Configuring IGMP Security Control

Configuration Effect

- Configure the range of multicast addresses that a user can access.
- Configure to allow a user from an unauthorized profile to preview a multicast channel.

- Configure the number of multicast addresses that a user can access.
- Configure to limit a user to receive only the multicast traffic from a router port to prevent illegal multicast traffic sent by the end user.
- Configure to limit a user to receive only the multicast traffic from designated source IP addresses to prevent illegal multicast traffic.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

▾ Configuring the Profile Filtering

- Optional.
- If you want to limit the profile packets to be received by a port, you can configure the profile filtering on the port.
- If you want to limit the multicast packets to be received by a VLAN, you can configure the per-VLAN profile filtering.

▾ Enabling Multicast Preview

- Optional.
- You can enable multicast preview for a user from an unauthorized profile.

▾ Configuring the Maximum Number of Profiles

- Optional.
- If you want to limit the number of multicast profiles that a port is allowed to receive, you can configure the maximum number of multicast profiles allowed for this port.
- If you want to limit the number of multicast profiles that global ports are allowed to receive, you can configure the maximum number of multicast profiles allowed for these ports.

Verification

- Run the **show ip igmp snooping interfaces** command to display the profile filtering and the maximum number of multicast profiles for a port.
- Run the **show ip igmp snooping vlan** command to display the per-VLAN profile filtering.
- Run the **show ip igmp snooping** command to check whether the maximum number of global multicast profiles, preview function, source port inspection, and source IP address inspection take effect.

Related Commands

▾ Configuring the Profile Filtering

Command	ip igmp snooping filter <i>profile-number</i>
Parameter	<i>profile-number</i> . Indicates a profile number.
Description	

Command Mode	Interface configuration mode
Usage Guide	N/A

↘ **Configuring the Per-VLAN Profile Filtering**

Command	ip igmp snooping vlan <i>vid</i> filter <i>profile-number</i>
Parameter Description	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094. <i>profile-number</i> : Indicates a profile number.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ **Configuring the Maximum Number of Profiles on a Port**

Command	ip igmp snooping max-groups <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of multicast profiles.
Command Mode	Interface configuration mode
Usage Guide	This value indicates only the number of dynamic multicast profiles, and the number of static profiles is not included. The counter of multicast profiles is based on the VLAN that the port belongs to. For example, if a port belongs to three VLANs, and all three of them receive a request packet from multicast profile 224.1.1.1 simultaneously, then the counter of multicast profiles will be 3 but not 1.

↘ **Configuring the Maximum Number of Global Profiles**

Command	ip igmp snooping l2-entry-limit <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of multicast profiles.
Command Mode	Global configuration mode
Usage Guide	This value includes the number of both dynamic profiles as well as static profiles.

↘ **Enabling Preview**

Command	ip igmp snooping preview <i>profile-number</i>
Parameter Description	<i>profile number</i> : Indicates the range of multicast addresses allowed for preview. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ **Configuring the Preview Duration**

Command	ip igmp snooping preview interval <i>num</i>
Parameter	<i>num</i> : Specifies the preview duration which ranges from 1s to 300s (60s by default).

Description	
Command Mode	Global configuration mode
Usage Guide	This configuration allows unauthorized users to receive multicast traffic within the preview duration. After the duration is met, the preview will be stopped; the preview can be resumed in 300s.

↳ [Displaying the Per-Port Profile Filtering](#)

Command	show ip igmp snooping interface
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the function is configured, the profile will be displayed, for example:</p> <pre> Orion Alpha A28X#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ----- GigabitEthernet 0/1 1 </pre>

↳ [Displaying the Per-VLAN Profile Filtering](#)

Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the function is configured, the profile will be displayed, for example:</p> <pre> IGMP VLAN filter: 1 </pre>

↳ [Displaying the Maximum Number of Interface Profiles](#)

Command	show ip igmp snooping interface
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the maximum number of multicast addresses for a port is configured, the value will be displayed, for example:</p> <pre> Orion Alpha A28X#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ----- </pre>

	GigabitEthernet 0/1	1	200
--	---------------------	---	-----

Displaying the Maximum Number of Global Profiles

Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the function is configured, the profile will be displayed, for example: <pre>IGMP Snooping L2-entry-limit: 65536</pre>

Displaying the Information of the Preview Function

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the range of multicast addresses for a port is configured, preview will be enabled, for example: <pre>IGMP Preview: Enable</pre> <pre>IGMP Preview group aging time : 60(Seconds)</pre>

Configuration Example

Configuring the Profile Filtering and the Maximum Number of Demanded Profiles

<p>Scenario Figure 2-9</p>	<p>The diagram illustrates a network topology for multicast configuration. Device A, a multicast router, is connected to Source 1 (IP 10.1.1.1/24) through its Gi 0/1 interface. Device A also has a Gi 0/2 interface connected to Device B, a Layer-2 device. Device B has three interfaces connected to receivers: Gi 0/2 to Receiver 1, Gi 0/3 to Receiver 2, and Gi 0/4 to Receiver 3. Both Device A and Device B have a VLAN 1 configured with IP 192.168.1.1.</p>
	<p>A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2.</p>

	<p>Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.</p> <p>By configuring VLAN 1, you can configure to allow the users within VLAN 1 to receive only the profiles whose addresses range from 225.1.1.1 to 225.1.255.255.</p> <p>You can configure Receiver 1 to receive only the profiles whose addresses range from 225.1.1.1 to 225.1.1.255, Receiver 2 to receive only the profiles whose addresses range from 225.1.2.1 to 255.1.2.255, and Receiver 3 to receive only the profiles whose addresses range from 225.1.3.1 to 225.1.3.255.</p> <p>At most 10 profiles can be added to a port and at most 100 profiles can be added globally.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode. ● Configure the range and maximum number of multicast addresses on B.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
<p>B</p>	<pre>B# configure terminal B(config)#ip igmp snooping ivgl B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#rang B(config-profile)#range 225.1.1.1 225.1.255.255 B(config-profile)#exit B(config)#ip igmp profile 2 B(config-profile)#permit B(config-profile)#range 225.1.1.1 225.1.1.255 B(config-profile)#exit B(config)#ip igmp profile 3 B(config-profile)#permit B(config-profile)#range 225.1.2.1 225.1.2.255</pre>

```

B(config-profile)#exit
B(config)#ip igmp profile 4
B(config-profile)#permit
B(config-profile)#range
B(config-profile)#range 225.1.3.1 225.1.3.255
B(config-profile)#exit
B(config)#ip igmp snooping l2-entry-limit 100
B(config)#ip igmp snooping vlan 1 filter 1
B(config)#int gigabitEthernet 0/2
Orion Alpha A28X(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 2
Orion Alpha A28X(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10
B(config)#int gigabitEthernet 0/3
Orion Alpha A28X(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 3
Orion Alpha A28X(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10
B(config)#int gigabitEthernet 0/4
Orion Alpha A28X(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 4
Orion Alpha A28X(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10

```

Verification

- Run the **show ip igmp snooping interfaces** command to display the profile filtering and the maximum number of multicast profiles for a port.
- Run the **show ip igmp snooping** command to display the maximum number of global multicast groups.

B

```

B#show ip igmp snooping interfaces

```

Interface	Filter profile number	max-group
GigabitEthernet 0/2	2	10
GigabitEthernet 0/3	3	10
GigabitEthernet 0/4	4	10

```

B#show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 100
Source port check: Disable
Source ip check: Disable

```


	IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)
--	---

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.
- The multicast router port is not learned, leading to failure to receive the multicast traffic.

2.4.6 Configuring an IGMP Profile

Configuration Effect

- Create an IGMP filtering profile.

Configuration Steps

↳ Creating a Profile

- (Optional) Create an IGMP filtering profile.

↳ Configuring the Profile Range

- (Optional) Configure the range of multicast profile addresses.

↳ Configuring the Profile Filtering

- (Optional) Configure the filtering mode of profile to **permit** or **deny**.

Verification

- Run the **show running-config** command to check whether the preceding configurations take effect.

Related Commands

↳ Creating a Profile

Command	ip igmp profile <i>profile-number</i>
Parameter Description	<i>profile-number</i> : Indicates the number of a profile.
Command Mode	Global configuration mode

Usage Guide	
--------------------	--

↘ [Configuring the Profile Range](#)

Command	range <i>low-ip-address</i> [<i>high-ip-address</i>]
Parameter	<i>low-ip-address</i> : Specifies the start address.
Description	<i>low-ip-address</i> : Specifies the end address. Only one address is configured by default.
Command Mode	Profile configuration mode
Usage Guide	You can configure multiple addresses. If the IP addresses of different ranges are consecutive, the addresses will be combined.

↘ [Configuring the Profile Filtering](#)

Command	deny
Parameter	N/A
Description	
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode of profile is set to deny while the range of multicast profiles is not specified, no profile is to be denied, which means to permit all profiles.

↘ [Configuring the Profile Filtering](#)

Command	permit
Parameter	N/A
Description	
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode of profile is set to permit while the range of multicast profiles is not specified, no profile is to be permitted, which means to deny all profiles.

[Configuration Example](#)

↘ [Creating a Filtering Profile](#)

Configuration Steps	<ul style="list-style-type: none"> ● Create a filtering profile. <pre>B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 224.1.1.1 235.1.1.1 B(config-profile)#</pre>
Verification	Run the show running-config command to check whether the configuration is successful.
	<pre>ip igmp profile 1 permit range 224.1.1.1 235.1.1.1 !</pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.
- The mode of profile is set to **permit** while the range of multicast profiles is not specified, leading to the denial of all profiles.

2.4.7 Configuring IGMP QinQ

Configuration Effect

- Create a multicast entry on the VLAN where IGMP packets are located. Forward IGMP packets on the VLAN where these packets are located, realizing transparent transmission.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↳ Configuring QinQ Transparent Transmission

- If the QinQ interface needs to forward multicast packets on the VLANs where the VIDs of the packets specify, enable QinQ to realize transparent transmission.

Verification

- Run the **show ip igmp snooping** command to check whether the configuration takes effect.

Related Commands

↳ Configuring QinQ Transparent Transmission

Command	ip igmp snooping tunnel
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable QinQ to realize transparent transmission of IGMP packets.

↳ Displaying QinQ Configuration

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed. <pre>IGMP Tunnel: Enable</pre>

Configuration Example

↳ Configuring QinQ Transparent Transmission

Configuration Steps	<ul style="list-style-type: none"> ● Configure basic IGMP snooping functions. ● Configure QinQ transparent transmission.
	<pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip igmp snooping tunnel Orion Alpha A28X(config)# Orion Alpha A28X(config)# end</pre>
Verification	Run the show ip igmp snooping command to check whether the configuration is successful.
	<pre>IGMP Tunnel: Enable</pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

2.4.8 Configuring an IGMP Querier

Configuration Effect

- Configure the device as an IGMP querier, which will send IGMP Query packets periodically and collect user demanding information.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↘ Enabling the Querier Function

- (Optional) Enable IGMP querier function globally or for a specified VLAN.
- (Optional) Disable the IGMP querier function for a specified VLAN.

↘ Configuring the Source IP Address of a Querier

- (Optional) You can configure the source IP address of a Query packet sent by the querier based on VLANs.
- After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect.

↘ Configuring the Maximum Response Time of a Query Packet

- (Optional) Adjust the maximum response time carried by an IGMP Query packet. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1.

↘ Configuring the Query Interval of a Querier

- (Optional) Adjust the interval of the IGMP querier for sending query packets.

↘ Configuring the Aging Timer of a Querier

- (Optional) Configure the aging timer of other IGMP queriers on the network.

↘ Specifying the IGMP Version for a Querier

- (Optional) Specify the IGMP version for a querier (IGMPv2 by default).

Verification

- Run the **show ip igmp snooping querier detail** command to check whether the configuration takes effect.

Related Commands

↘ Enabling the IGMP Querier Function

Command	ip igmp snooping [vlan vid] querier
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	IGMP querier for a specified VLAN will take effect only after global IGMP querier is enabled. If global IGMP querier is disabled, IGMP querier for all the VLANs will be disabled.

↘ Configuring the Source IP Address of a Querier

Command	ip igmp snooping [vlan vid] querier address a.b.c.d
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. a.b.c.d: Indicates the source IP address.

Command Mode	Global configuration mode
Usage Guide	After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect. If the source IP address is specified by a VLAN, the address will be used preferentially.

↘ Configuring the Maximum Response Time of a Querier

Command	ip igmp snooping [vlan vid] querier max-response-time seconds
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. seconds: Indicates the maximum response time. in the unit of seconds. The value ranges from 1 to 25.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

↘ Configuring the Query Interval of a Querier

Command	ip igmp snooping [vlan vid] querier address a.b.c.d
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. seconds: Indicates the query interval in the unit of seconds. The value ranges from 1 to 18,000.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

↘ Configuring the Aging Timer of a Querier

Command	ip igmp snooping [vlan vid] querier timer expiry seconds
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. seconds: Indicates the timeout time in the unit of seconds. The value ranges from 60 to 300.
Command Mode	Global configuration mode
Usage Guide	A device may fail to be elected as the querier even when its querier function is enabled. If a device that fails to be elected does not receive the Query packet sent by the querier in the aging time, the querier in use is considered as expired, and a new round of election will be raised. If the aging time is specified by a VLAN, the value will be used preferentially.

↘ Specifying the IGMP Version for a Querier

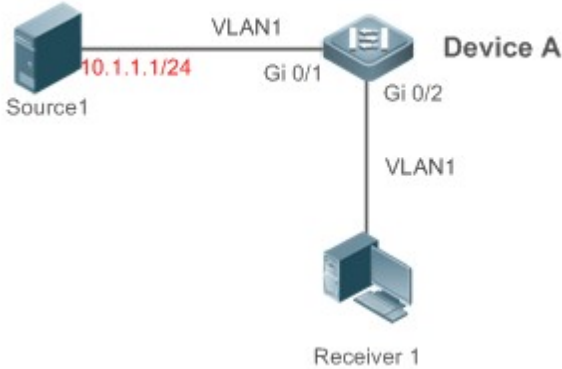
Command	ip igmp snooping [vlan vid] querier version 1
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A querier can be run in IGMPv1 and IGMPv2 (IGMPv2 by default). You can also run a command to configure the version to IGMPv1. If the IGMP version for a querier is specified by a VLAN, the version will be used preferentially.

↳ Displaying the IGMP Querier Configuration

Command	show ip igmp snooping querier detail
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If QinQ is enabled, the following content is displayed.</p> <pre>Orion Alpha A28X(config)#show ip igmp snooping querier detail Vlan IP Address IGMP Version Port ----- Global IGMP switch querier status ----- admin state : Enable admin version : 2 source IP address : 1.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 Vlan 1: IGMP switch querier status ----- admin state : Disable admin version : 2 source IP address : 1.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 operational state : Disable operational version : 2</pre>

Configuration Example

↳ Enabling the IGMP Querier Function

<p>Scenario Figure 2-10</p>	 <p>The diagram illustrates a network topology. On the left, a server icon labeled 'Source1' is connected to a central switch icon labeled 'Device A'. The connection is labeled 'VLAN1' and 'Gi 0/1'. The IP address '10.1.1.1/24' is shown in red text near Source1. On the right, 'Device A' is connected to a laptop icon labeled 'Receiver 1'. This connection is also labeled 'VLAN1' and 'Gi 0/2'.</p>
	<p>In the scenario without Layer-3 multicast equipment, the multicast traffic can be forwarded only on the Layer-2 network. A acts as a Layer-2 device to connect to the multicast source and receiver.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Enable global IGMP snooping on A in IVGL mode. ● Enable IGMP querier for VLAN 1 on A.
<p>A</p>	<pre>A(config)#ip igmp snooping ivgl A(config)#ip igmp snooping querier A(config)#ip igmp snooping querier address 10.1.1.1 A(config)#ip igmp snooping vlan 1 querier</pre>
<p>Verification</p>	<p>Run the show ip igmp snooping querier command to check whether the querier of VLAN 1 takes effect.</p>
<p>A</p>	<pre>A(config)#show ip igmp snooping querier Vlan IP Address IGMP Version Port ----- 1 10.1.1.1 2 switch A(config)#show ip igmp snooping querier vlan 1 Vlan 1: IGMP switch querier status ----- elected querier is 10.1.1.1 (this switch querier) ----- admin state : Enable admin version : 2</pre>


```

source IP address      : 10.1.1.1
query-interval (sec)  : 60
max-response-time (sec) : 10
querier-timeout (sec) : 125
operational state     : Querier
operational version   : 2

```

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

2.5 Monitoring

Clearing

- Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the statistics on IGMP snooping.	clear ip igmp snooping statistics
Clears the dynamic router ports and member ports.	clear ip igmp snooping gda-table

Displaying

Description	Command
Displays basic IGMP snooping configurations.	show ip igmp snooping [vlan <i>vlan-id</i>]
Displays the statistics on IGMP snooping.	show ip igmp snooping statistics [vlan <i>vlan-id</i>]
Displays the router ports.	show ip igmp snooping mrouter
Displays the IGMP snooping entries.	show ip igmp snooping gda-table
Displays the profile.	show ip igmp profile [<i>profile-number</i>]
Displays the IGMP snooping configurations on an interface.	show ip igmp snooping interface <i>interface-name</i>
Displays the IGMP querier.	show ip igmp snooping querier [detail]

Debugging

- System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs all IGMP Snooping functions.	debug igmp-snp
Debugs the IGMP snooping events.	debug igmp-snp event
Debugs the IGMP snooping packets.	debug igmp-snp packet

Debugs the communications between IGMP snooping and MSF.	debug igmp-snp msf
Debugs the IGMP snooping alarms.	debug igmp-snp warning