Contents

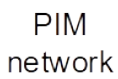
1 Configuring IGMP Snooping

1.1 Introduction

Internet Group Management Protocol (IGMP) snooping is a process of snooping protocol packets between an L3 multicast device and hosts to manage and control forwarding of IP multicast traffic at the data link layer, implementing L2 multicast.

Generally, multicast packets need to pass through L2 switches, especially in some local area networks (LANs). As shown in Figure 1-1, the Protocol Independent Multicast (PIM) multicast device sends packets to hosts through an L2 switch. Because multicast group addresses cannot be learned on L2 devices, the packets will be broadcast in the VLAN. This wastes bandwidth and affects security. After the IGMP snooping function is configured, the L2 switch can listen to IGMP packets between hosts and the uplink PIM multicast device and establish L2 multicast forwarding entries to ensure that multicast data is forwarded only to specific hosts. This prevents multicast data from being broadcast in the L2 network.

Figure 1-1 Network Topology



1.1.2 Principles

IGMP snooping is a basic L2 multicast function that forwards and controls multicast data at the data link layer. By listening to and analyzing protocol packets between hosts and the L3 multicast device, the L2 device running IGMP snooping establishes and maintains L2 multicast forwarding entries to ensure on-demand forwarding of multicast data at the link layer.

As shown in Figure 1-1, when IGMP snooping is not configured on the L2 device, IP multicast packets are broadcast in the VLAN. As shown in Figure 1-2, when IGMP snooping is enabled on the L2 device, IP multicast packets are forwarded only to the member hosts of the multicast group. This prevents multicast data from being broadcast in the L2 network.

Figure 1-1 Multicast Data Transmission When IGMP Snooping Is Disabled

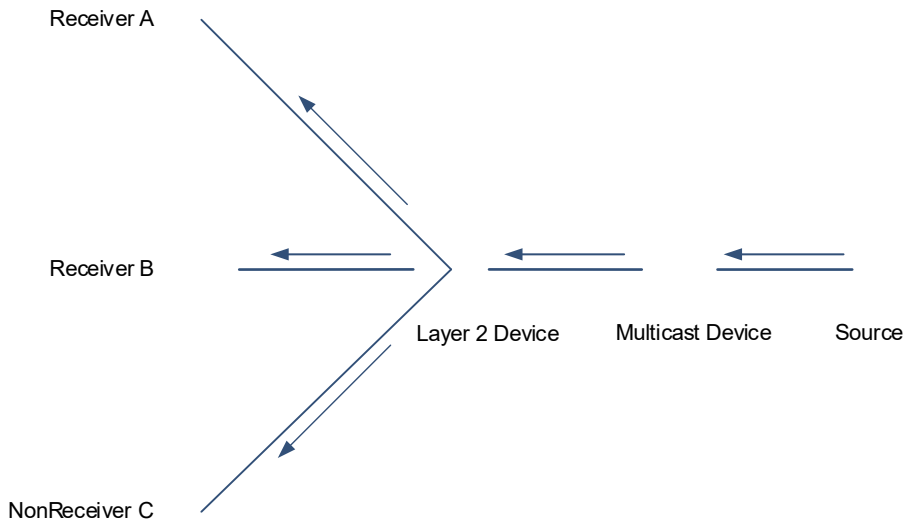
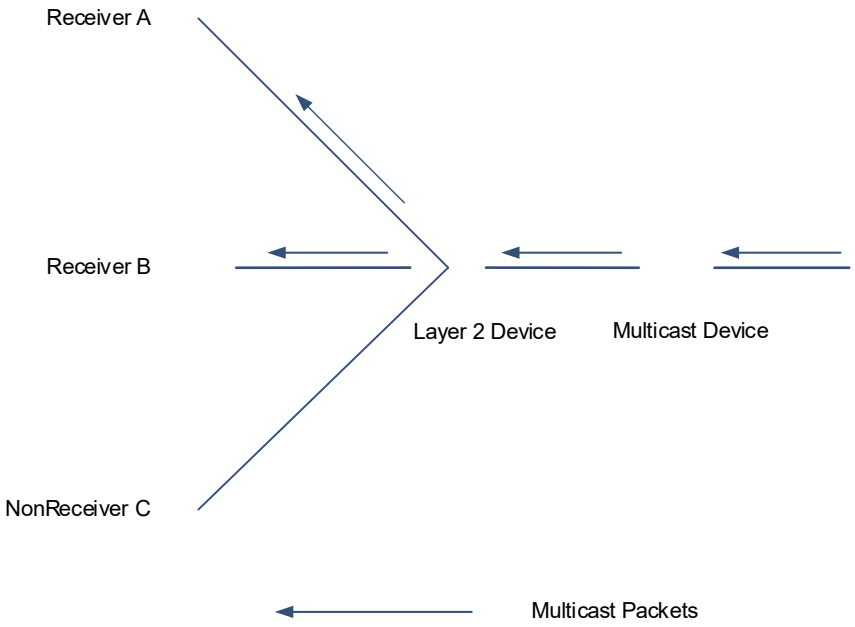


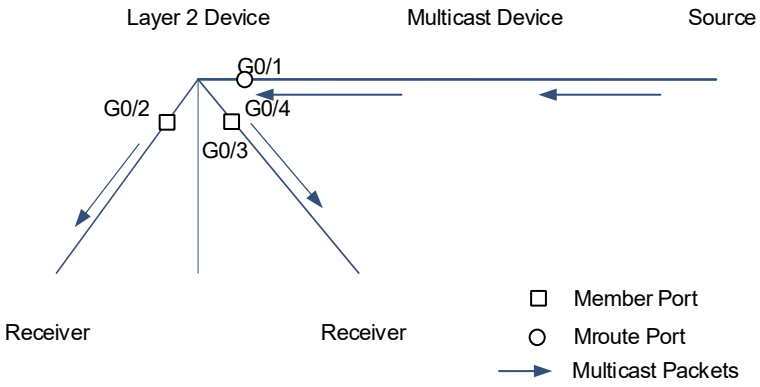
Figure 1-2 Multicast Data Transmission When IGMP Snooping Is Enabled



1.1.3 Port Types

IGMP snooping is enabled on a per-VLAN basis. IGMP snooping ports are ports in a VLAN. The device running IGMP snooping identifies ports in a VLAN as multicast router ports or member ports to manage and control forwarding of IP multicast data in the VLAN.

Figure 1-1 IGMP Snooping Ports



- A multicast router port connects the L2 multicast device to an L3 multicast device, and indicates the direction of the multicast source. By listening to IGMP packets, the L2 multicast device can automatically discover and maintain dynamic multicast router ports. You can also configure static multicast router ports.
- A member port connects the L2 multicast device to a host in a multicast group, and indicates the direction of a multicast group member. It is also called a listener port. By listening to IGMP packets, the L2 multicast device can automatically discover and maintain dynamic member ports. You can also configure static member ports.

As shown in Figure 1-1, IGMP snooping is enabled on the L2 multicast device, and the multicast data is received from a multicast router port and sent out from a member port.

1.1.4 Working Mechanism

A device running IGMP snooping analyzes received IGMP packets to discover and identify multicast router ports and member ports and establish and maintain IGMP snooping forwarding entries. The device can identify and process the following types of IGMP packets:

1. Query Packets

The IGMP querier periodically sends a general Query packet, and sends a group-specific Query packet when it receives a Leave packet. When the device running IGMP snooping receives a Query packet, the device performs the following actions in the VLAN:

- The device forwards the IGMP Query packet through all ports (except the port receiving the packet).
- If the port receiving the Query packet is a dynamic multicast router port, the device resets the aging timer of the port. After the timer times out, the port is no longer used as a dynamic multicast router port.
- If the port receiving the Query packet is not a dynamic multicast router port, the device uses the port as the dynamic multicast router port and starts the aging timer. After the timer times out, the port is no longer used as a dynamic multicast router port.
- If the function of dynamical multicast router port learning is disabled, the device will not learn dynamic multicast router ports.

2. Report Packets

When a member host receives a Query packet, the host will respond with a Report packet. If a host wants to join a multicast group, the host will proactively send a Report packet. The device running IGMP snooping can process IGMPv1 and IGMPv2 packets by default. For Report packets of IGMPv3, the device only processes the group information and does not process the carried source information.

When the device running IGMP snooping receives a Report packet, the device performs the following actions in the VLAN:

- The device forwards the Report packet through all multicast router ports. If Report packet suppression is enabled on the device, the device forwards only the first Report packet of each group in an IGMP query interval.
- If the port receiving the Report packet is a dynamic member port, the device resets the aging timer of the port. After the timer times out, the port is no longer used as a dynamic member port.
- If the port receiving the Report packet is not a member port, the device uses the port as the dynamic member port and starts the aging timer. After the timer times out, the port is no longer used as a dynamic member port.

3. Leave Packets

If a host wants to leave a multicast group, the host will proactively send a Leave packet. When the device running IGMP snooping receives a Leave packet, the device performs the following actions in the VLAN:

- The device forwards the Leave packet through all multicast router ports.
- If the port receiving the Leave packet is a dynamic member port and the fast leave function is configured,

the device immediately deletes the port from the IGMP snooping forwarding entry of the corresponding multicast group. The port is no longer used as a dynamic member port of the group.

- If the port receiving the Leave packet is a dynamic member port but the fast leave function is not configured, the port status remains unchanged. When the aging timer of the port times out, the device deletes the port from the IGMP snooping forwarding entry of the corresponding multicast group. The port is no longer used as a dynamic member port of the group.

1.1.5 Protocols and Standards

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

1.2 Configuration Task Summary

IGMP snooping configuration includes the following tasks:

(1) Configuring Basic IGMP Snooping Functions. Select either of the following configuration tasks to configure.

- Configuring Basic IGMP Snooping Functions in IVGL Mode
- Configuring Basic IGMP Snooping Functions in SVGL Mode
- Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

(2) Configuring Protocol Packet Processing Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Static Multicast Router Port
- Configuring a Static Member Port
- Configuring Report Packet Suppression
- Configuring Port Fast Leave
- Configuring Dynamic Multicast Router Port Learning
- Configuring the Aging Time for Dynamic Multicast Router Ports
- Configuring the Aging Time for Dynamic Member Ports

(3) (Optional) Configuring IGMP Snooping Querier. The tasks are as follows:

- Enabling IGMP Snooping Querier
- Configuring the Source IP Address of a Querier
- (Optional) Configuring the IGMP Snooping Querier Version
- (Optional) Configuring the Maximum Response Time for Query Packets
- (Optional) Configuring the Interval for a Querier to Send Query Packets
- (Optional) Configuring the Querier Aging Time

(4) Configuring Multicast Security Control. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring a Range of Multicast Group Addresses for a Profile

-
- Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request
- Configuring Source Port Check
- Configuring Source IP Address Check

(5) (Optional) Configuring QinQ Processing

1.3 Configuring Basic IGMP Snooping Functions

1.3.1 Overview

The device running IGMP snooping can provide independent or shared multicast services for user VLANs when operated in the following modes:

- Independent VLAN Group Learning (IVGL): provides independent multicast services for each user VLAN.
- Shared VLAN Group Learning (SVGL): provides shared multicast services for multiple user VLANs.
- IVGL-SVGL: provides both shared and independent multicast services for user VLANs.

1.3.2 Restrictions and Guidelines

- The SVGL mode and the IP multicast function are mutually exclusive. If the IP multicast function needs to be enabled on the device running IGMP snooping, the device can operate only in IVGL mode.
- If the device running IGMP snooping operates in SVGL or IVGL-SVGL mode, the multicast groups associated with the SVGL mode must be configured. First, define the multicast groups applied in the SVGL mode in a profile. Then, apply this profile in the command for configuring the group range in SVGL mode.

1.3.3 Configuration Tasks

Basic IGMP snooping function configuration includes the following tasks. Please configure only one task.

- Configuring Basic IGMP Snooping Functions in IVGL Mode
- Configuring Basic IGMP Snooping Functions in SVGL Mode
- Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

1.3.4 Configuring Basic IGMP Snooping Functions in IVGL Mode

1. Overview

In IVGL mode, the device running IGMP snooping provides independent multicast services for each user VLAN. Multicast traffic can be forwarded only in the belonged VLAN, and hosts can request multicast traffic only in the belonged VLAN.

2. Restrictions and Guidelines

- Unless otherwise specified, you are advised to enable IGMP snooping globally on all L2 access devices connecting to hosts.
- After IGMP snooping is enabled globally, it takes effect to all VLANs. You can disable IGMP snooping on any VLAN. When the multicast service is disabled on a VLAN, the multicast services on other VLANs are not affected.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IGMP snooping globally and run the IVGL mode.

ip igmp snooping ivgl

IGMP snooping is disabled by default.

(4) (Optional) Disable IGMP snooping on a VLAN.

no ip igmp snooping vlan *vlan-id*

After IGMP snooping is enabled globally, it takes effect to all VLANs by default.

If IGMP snooping is disabled globally, it is ineffective on all VLANs.

You can disable IGMP snooping on a VLAN only after IGMP snooping is enabled globally.

1.3.5 Configuring Basic IGMP Snooping Functions in SVGL Mode

1. Overview

In SVGL mode, the device running IGMP snooping can provide shared multicast services for multiple user VLANs. Shared multicast services are usually used to provide the same video on demand (VOD) service for users in multiple VLANs. Compared with independent multicast services, shared multicast services save bandwidth.

VLANs for shared multicast services are classified into a shared VLAN and sub VLANs. Multicast traffic of multicast groups applied in SVGL mode on the shared VLAN is forwarded from the shared VLAN to sub VLANs, and hosts on sub VLANs request multicast traffic of multicast groups applied in SVGL mode from the shared VLAN.

2. Restrictions and Guidelines

- To share multicast services among VLANs, you need to configure multicast groups applied in SVGL mode after configuring the SVGL mode.
- Shared multicast services apply only to the shared VLAN and sub VLANs and use group addresses applied in SVGL mode.

3. Prerequisites

Before configuring multicast groups associated with the SVGL mode, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IGMP snooping globally and run the SVGL mode.

ip igmp snooping svgl

IGMP snooping is disabled by default.

(4) Configure multicast groups associated with the SVGL mode.

ip igmp snooping svgl profile *profile-number*

No multicast group is associated with the SVGL mode by default.

(5) (Optional) Specify a shared VLAN.

ip igmp snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

(6) (Optional) Specify sub VLANs in SVGL mode.

ip igmp snooping svgl subvlan *vlan-range*

By default, all VLANs except the shared VLAN are sub VLANs in SVGL mode.

1.3.6 Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

1. Overview

The IVGL-SVGL mode is also called the hybrid mode. In IVGL-SVGL mode, the device running IGMP snooping can provide both shared and independent multicast services for user VLANs.

- In the shared VLAN and sub VLANs, shared multicast services apply to the multicast traffic of multicast groups applied in SVGL mode, and independent multicast services apply to other multicast traffic.
- In other VLANs (except the shared VLAN and sub VLANs), independent multicast services are provided.

2. Restrictions and Guidelines

- After configuring the IVGL-SVGL mode, you must specify the multicast groups associated with the SVGL mode.
- When a user VLAN is configured as a shared VLAN or sub VLAN, the user VLAN enjoys both shared and independent multicast services. When a user VLAN is configured as other VLANs, it enjoys only independent multicast services.

3. Prerequisites

Before configuring multicast groups associated with the SVGL mode, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IGMP snooping globally and run the IVGL-SVGL mode.

ip igmp snooping ivgl-svgl

IGMP snooping is disabled by default.

(4) Configure multicast groups associated with the SVGL mode.

ip igmp snooping svgl profile *profile-number*

No multicast group is associated with the SVGL mode by default.

(5) (Optional) Specify a shared VLAN.

ip igmp snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

(6) (Optional) Specify sub VLANs in SVGL mode.

ip igmp snooping svgl subvlan *vlan-range*

All VLANs except the shared VLAN are sub VLANs in SVGL mode by default.

1.4 Configuring Protocol Packet Processing Parameters

1.4.1 Overview

By controlling protocol packet processing, an L2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and IGMP snooping membership quickly.

1.4.2 Restrictions and Guidelines

Configuring Basic IGMP Snooping Functions Related configuration functions take effect only after basic IGMP snooping functions are configured.

1.4.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Static Multicast Router Port
- Configuring a Static Member Port
- Configuring Report Packet Suppression
- Configuring Port Fast Leave
- Configuring Dynamic Multicast Router Port Learning
- Configuring the Aging Time for Dynamic Multicast Router Ports
- Configuring the Aging Time for Dynamic Member Ports

1.4.4 Configuring a Static Multicast Router Port

1. Overview

A multicast router port is used to receive uplink multicast data and forward IGMP Report and Leave packets. Static multicast router ports never age and can forward IGMP Report and Leave packets to the uplink IGMP querier stably.

2. Restrictions and Guidelines

- In SVGL mode, if no sub VLAN is configured, the configuration of static multicast router ports is valid only in the shared VLAN. In other VLANs, static multicast router ports can be configured but do not take effect. If sub VLANs are configured, the configuration of static multicast router ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static multicast router ports can be configured but do not take effect.
- In SVGL-IVGL mode, if no sub VLAN is configured, the configuration of static multicast router ports is valid in all VLANs. If sub VLANs are configured, the configuration of static multicast router ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static multicast router ports can be configured but do not take effect.
- In IVGL mode, the configuration of static multicast router ports is valid in all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static multicast router port.

ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

No static multicast router port is configured by default.

1.4.5 Configuring a Static Member Port

1. Overview

When a member port connecting to a member host is configured as a static member port, the host can receive multicast traffic from the specified multicast group no matter whether the host joins the multicast group. Static member ports never age.

2. Restrictions and Guidelines

- In SVGL mode, if no sub VLAN is configured, the configuration of static member ports is valid only in the shared VLAN. In other VLANs, static member ports can be configured but do not take effect. If sub VLANs are configured, the configuration of static member ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static member ports can be configured but do not take effect.
- In SVGL-IVGL mode, if no sub VLAN is configured, the configuration of static member ports is valid in all VLANs. If sub VLANs are configured, the configuration of static member ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static member ports can be configured but do not take effect.
- In IVGL mode, the configuration of static member ports is valid in all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static member port.

ip igmp snooping vlan *vlan-id* **static** *group-address* **interface** *interface-type interface-number*

No static member port is configured by default.

1.4.6 Configuring Report Packet Suppression

1. Overview

IGMP Query and Report packets are exchanged periodically to maintain the group membership. When many hosts in a network join the same multicast group, a large number of IGMP packets will be sent to the IGMP multicast device, which wastes network bandwidth and affects the performance of the IGMP multicast device. Report packet suppression can optimize this situation.

When Report packet suppression is configured, the IGMP multicast device only forwards the first Report packet from a specific VLAN for a multicast group to the multicast router port and suppresses subsequent Report packets for the same multicast group during one query interval. This function reduces the number of packets in the network.

2. Restrictions and Guidelines

Only IGMPv1 and IGMPv2 Report packets can be suppressed, and IGMPv3 Report packets cannot be suppressed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure Report packet suppression.

ip igmp snooping suppression enable

Report packet suppression is disabled by default.

1.4.7 Configuring Port Fast Leave

1. Overview

When the port fast leave function is enabled and a port receives a Leave packet (including the IGMPv2 Leave packet and IGMPv3 Report packet of the INCLUDE type without carrying any source address), the port is directly deleted from the member port list of the corresponding multicast forwarding entry. When receiving group-specific Query packets and multicast data, the device does not forward the packets to this port.

2. Restrictions and Guidelines

The port fast leave function is applicable when only one host is connected to each port. This function helps save bandwidth and resources.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the port fast leave function.

ip igmp snooping fast-leave enable

The port fast leave function is disabled by default.

1.4.1 Configuring Dynamic Multicast Router Port Learning

1. Overview

In some application scenarios, a user host may send Query packets and PIM neighbor messages. When the L2 device receives such Query packets or PIM neighbor messages, the L2 device will set the port receiving the packets as a dynamic multicast router port. All multicast packets in the VLAN will be forwarded to this port, and the host receives a large number of useless multicast packets. In addition, Query packets and PIM neighbor messages sent by user hosts may affect the status of the L3 multicast routing protocol, such as the querier and designated router (DR) election. In this case, you can disable dynamic multicast router port learning to resolve this problem and improve network security.

2. Restrictions and Guidelines

Disabling dynamic multicast router port learning and enabling a static multicast router port do not affect each other.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure dynamic multicast router port learning.

ip igmp snooping [**vlan** *vlan-id*] **mrouter learn pim-dvmrp**

Dynamic multicast router port learning is enabled by default.

1.4.2 Configuring the Aging Time for Dynamic Multicast Router Ports

1. Overview

A multicast router port is used to receive uplink multicast data and forward IGMP Report and Leave packets. After enabling IGMP snooping, an L2 device can dynamically learn multicast router ports to forward multicast packets for the unplink device. If a dynamic multicast router port does not receive a Query packet or neighbor message from the uplink device within the aging time due to unstable network or packet congestion, the L2 device will delete the dynamic multicast router port, which may cause multicast data interruption.

2. Restrictions and Guidelines

- You can adjust the aging time of dynamic multicast router ports based on the network load. When the network load is heavy, set the aging time to a larger value. A too short aging time may cause dynamic multicast router ports to be added and deleted frequently, resulting in data interruption.
- You can set the aging time based on the interval for the connected multicast router to send IGMP Query packets. Generally, the aging time is set to twice the interval plus the response time of the last IGMP Query packet.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for dynamic multicast router ports.

ip igmp snooping dyn-mr-aging-time *dynamic-mroute-aging-time*

The default aging time of dynamic multicast router ports is 300s.

1.4.3 Configuring the Aging Time for Dynamic Member Ports

1. Overview

When the device running IGMP snooping receives an IGMP Join packet from a host to join an IP multicast group, the device adds the port receiving the packet to the member port list and sets an aging time for the port. If the port is already in the member port list, the device resets the aging timer of the port. After the timer times out, it is deemed that no user host receives multicast packets through this port, and the multicast device deletes the port from the IGMP snooping member port list.

2. Restrictions and Guidelines

- You can adjust the aging time of dynamic member ports based on the network load. When the network load is heavy, set the aging time to a larger value. A too short aging time may cause dynamic member ports to be added and deleted frequently, resulting in data interruption.
- After the aging time is configured, the aging timer value of dynamic member ports is *host-aging-time* for subsequent IGMP Join packets. The configured aging time takes effect after the next Join packet is received, and the started member port aging timers are not updated.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for dynamic member ports.

ip igmp snooping host-aging-time *host-aging-time*

The default aging time of dynamic member ports is 260s.

1.5 Configuring IGMP Snooping Querier

1.5.1 Overview

In a three-layer multicast network, the L3 multicast device serves as the querier and runs IGMP to maintain group membership. The L2 multicast device only needs to listen to IGMP packets to establish and maintain multicast forwarding entries, implementing L2 multicast. When a multicast source and user host are in the same L2 network, the query function is unavailable because the L2 device does not support IGMP. To resolve this problem, you can enable the IGMP snooping querier function on the L2 device so that the L2 device sends IGMP Query packets to user hosts on behalf of the L3 multicast device, and listens to and maintains IGMP Report packets responded by user hosts to establish L2 multicast forwarding entries. When multiple devices are configured as the querier in the L2 network and a device receives IGMP Query packets from other devices, an IGMP snooping querier is elected.

1.5.2 Restrictions and Guidelines

- After the querier function is enabled, you must specify a source IP address for the querier so that the querier function can take effect.
- When a device with the querier function enabled receives a PIM or Distance Vector Multicast Routing Protocol (DVMRP) packet, it regards that a multicast router exists in the network. To prevent the IGMP routing function of the multicast router from being affected, the querier function of the device becomes invalid and the multicast router in the network serves as the IGMP snooping querier.
- The query interval configured for the querier must be greater than the maximum response time of Query packets. Otherwise, the configuration fails.

1.5.3 Prerequisites

Configuring Basic IGMP Snooping Functions

1.5.4 Configuration Tasks

IGMP snooping querier configuration includes the following tasks:

- Enabling IGMP Snooping Querier
- Configuring the Source IP Address of a Querier
- (Optional) Configuring the IGMP Snooping Querier Version
- (Optional) Configuring the Maximum Response Time for Query Packets
- (Optional) Configuring the Interval for a Querier to Send Query Packets
- (Optional) Configuring the Querier Aging Time

1.5.5 Enabling IGMP Snooping Querier

1. Overview

After the IGMP snooping querier function is enabled on an L2 device, the L2 device sends IGMP Query packets to user hosts on behalf of the L3 device.

2. Restrictions and Guidelines

- The IGMP snooping querier function must be enabled globally and on a specific VLAN. The IGMP snooping querier function on a specific VLAN takes effect only after the function is enabled globally.
- You can disable the IGMP snooping querier function for a specific VLAN.
- If the IGMP snooping querier function is disabled globally, the function is disabled on all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IGMP snooping querier function.

ip igmp snooping [**vlan** *vlan-id*] **querier**

The IGMP snooping querier function is disabled by default.

1.5.6 Configuring the Source IP Address of a Querier

1. Overview

You can configure the source IP address of a querier globally or on a specific VLAN. If the source IP address of the querier is not configured, the querier function does not take effect.

2. Restrictions and Guidelines

The querier source IP address configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the source IP address of a querier.

ip igmp snooping [**vlan** *vlan-id*] **querier address** *source-address*

By default, no VLAN is specified, and the source IP address configuration applies to all VLANs.

1.5.7 Configuring the IGMP Snooping Querier Version

1. Overview

You can configure the IGMP snooping querier version to specify the version of IGMP Query packets sent by the querier. The supported IGMP versions include IGMPv1and IGMPv2.

2. Restrictions and Guidelines

- An IGMP snooping querier supports IGMPv1and IGMPv2, and IGMPv2 is used by default. You can run the

corresponding command to enable an IGMP snooping querier to run IGMPv1 or IGMPv3.

- The IGMP snooping querier version configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IGMP snooping querier version.

ip igmp snooping [**vlan** *vlan-id*] **querier version 1**

An IGMP snooping querier runs IGMPv2 by default.

1.5.8 Configuring the Maximum Response Time for Query Packets

1. Overview

When hosts in the directly-connected network segment of the device serving as the IGMP snooping querier receive a Query packet from the device, the hosts need to return a Report packet within the maximum response time. This function allows you to configure the maximum response time for Query packets on the device. If no host returns a Report packet within the maximum response time, the device considers that no group member exists in the directly-connected network segment and deletes the group information.

2. Restrictions and Guidelines

- You can adjust the maximum response time for Query packets based on the network load. When the network load is light, you are advised to set the maximum response time for Query packets to a small value to enable hosts to make quick responses to IGMP Query packets. When the network load is heavy, set a large maximum response time to avoid network congestion due to flooding of Report packets sent by hosts after the timer times out.
- Because IGMPv1 does not support carrying the maximum response time in packets, this configuration does not take effect to a querier running IGMPv1.
- You can configure different maximum response time values for queriers in different VLANs. The maximum response time configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum response time for Query packets.

ip igmp snooping [**vlan** *vlan-id*] **querier max-response-time** *max-response-time*

The maximum response time for Query packets is 10s by default.

1.5.9 Configuring the Interval for a Querier to Send Query Packets

1. Overview

An IGMP snooping querier periodically sends Query packets. This parameter is used to define the interval for sending Query packets.

2. Restrictions and Guidelines

You can configure the interval for a querier to send Query packets globally or on a specific VLAN. The query interval specified on a VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interval for a querier to send Query packets.

ip igmp snooping [**vlan** *vlan-id*] **querier query-interval** *query-interval*

The default interval for an IGMP snooping querier to send Query packets is 60s.

1.5.10 Configuring the Querier Aging Time

1. Overview

When multiple queriers are configured in an L2 network, querier election will be performed, and the device elected as the querier will send Query packets periodically. Other candidate queriers receive Query packets from the elected querier. If a candidate querier does not receive Query packets from the elected querier within a specific period of time, the candidate querier regards that it is the only querier in the directly-connected network segment and initiates a new round querier election. This parameter is used to define the timeout time for candidate queriers to receive Query packets from the elected querier.

2. Restrictions and Guidelines

The querier aging time configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the querier aging time.

ip igmp snooping [**vlan** *vlan-id*] **querier timer expiry** *timeout*

The default aging time of IGMP snooping queriers is 125s.

1.6 Configuring Multicast Security Control

1.6.1 Overview

After multicast security control is configured, the device running IGMP snooping can control the multicast service scope and load to prevent invalid multicast traffic and improve L2 multicast network security.

1.6.2 Prerequisites

Configuring Basic IGMP Snooping Functions

1.6.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring a Range of Multicast Group Addresses for a Profile
-
- **Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request**
- Configuring Source Port Check
- Configuring Source IP Address Check

1.6.4 Configuring a Profile

1. Overview

A profile is used to define a range of multicast groups that permit or deny user access for reference by other functions.

- When the SVGL mode is enabled, a profile is used to define a range of multicast groups applied in SVGL mode.
- When multicast filtering is configured on a port, a profile is used to define a range of multicast groups that permit or deny user access through the port.
- When multicast filtering is configured on a VLAN, a profile is used to define a range of multicast groups that permit or deny user access on the VLAN.
- When the preview function is enabled, a profile is used to define a range of multicast groups to be previewed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a profile.

ip igmp profile *profile-number*

No profile is created by default.

(4) Define a range of multicast groups for a profile.

range *low-ip-address* [*high-ip-address*]

No multicast group range is defined for a profile by default.

Multiple multicast group ranges can be configured at the same time. If two multicast group ranges overlap, the ranges will be merged automatically.

(5) Configure the filtering action for a profile. The configuration steps below are mutually exclusive. Please configure only one task.

- Set the filtering action of a profile to Deny.

  deny

  If only the Deny action is configured and no multicast group range is configured, no group is denied. The effect is the same as permitting all groups.

- (Optional) Set the filtering action of a profile to Permit.

  permit

  If only the Permit action is configured and no multicast group range is configured, no group is permitted. The effect is the same as denying all groups.

The Deny action is performed for a profile by default.

1.6.5 Configuring a Range of Multicast Group Addresses for a Profile

1. Overview

Generally, the device running ports and VLANs can join any multicast group. By configuring a range of multicast groups that permit or deny user access, you can customize the multicast service scope for users to guarantee the interest of operators and prevent invalid multicast traffic.

2. Restrictions and Guidelines

- By applying a profile to a VLAN, you can restrict the multicast groups that users can join in the VLAN.
- By applying a profile to a port, you can restrict the multicast groups that users can join on the port.

3. Prerequisites

Before configuring a range of multicast group addresses for a profile, ensure that the corresponding profile is created and a range of multicast groups is specified for the profile. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

Configure a range of multicast groups for a profile. Select at least one of them to configure.

- Apply a profile for a port.

  a Enter the privileged EXEC mode.

  enable

  b Enter the global configuration mode.

  configure terminal

  c Enter the interface configuration mode.

  interface *interface-type interface-number*

d Apply a profile to a port.

ip igmp snooping filter *profile-number*

No profile is applied to a port by default.

- Apply a profile to a VLAN.

a Enter the privileged EXEC mode.

enable

e Enter the global configuration mode.

configure terminal

f Apply a profile to a VLAN.

ip igmp snooping vlan *vlan-id* **filter** *profile-number*

No profile is applied to a VLAN by default.

1.6.6 Configuring Multicast Preview

1. Overview

In video applications, the administrator configures a VLAN filter or port filter to control some premium channels. Users who do not subscribe to these channels cannot watch these channels on demand. The multicast preview function allows unpaid users to preview premium channels before they decide whether to pay for watching. This function can be used together with multicast permission control.

2. Restrictions and Guidelines

After the preview duration ends, unpaid users can no longer watch premium channels on demand. The previewed content can be previewed again after 300s.

3. Prerequisites

Before configuring multicast preview, ensure that the corresponding profile is created and a range of multicast groups allowed for preview is specified. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure multicast preview.

ip igmp snooping preview *profile-number*

The multicast preview function is disabled by default.

(4) (Optional) Configure the preview duration.

ip igmp snooping preview interval preview-*interval*

The default multicast preview duration is 60s.

1.6.7 Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request

1. Overview

If too much multicast traffic is requested concurrently, the multicast device will be severely burdened. Configuring the maximum number of multicast groups allowed for concurrent request can guarantee the bandwidth. You can limit the number of multicast groups allowed for concurrent request globally or on a port.

- Global maximum number of multicast groups allowed for concurrent request: This configuration contains statically configured and dynamically learned multicast groups.
- Maximum number of multicast groups allowed for concurrent request on a port: This configuration contains only dynamically learned multicast groups on a port and does not include statically configured multicast groups.

2. Restrictions and Guidelines

- To limit the number of multicast groups allowed for concurrent request globally, configure the global maximum number of multicast groups allowed for concurrent request.
- To limit the number of multicast groups allowed for concurrent request on a port, configure the maximum number of multicast groups that can be dynamically learned by the port.
- The number of multicast groups that can be dynamically learned by a port is counted based on the VLANs to which the port belongs. For example, if a port belongs to three VLANs and the port receives requests of multicast group 224.1.1.1 from each VLAN, the multicast group count on the port is 3 instead of 1.

3. Procedure

Configure the maximum number of multicast groups allowed for concurrent request. Select at least one of them to configure.

- Configure the maximum number of multicast groups allowed for concurrent request globally.
  a Enter the privileged EXEC mode.
  enable
  b Enter the global configuration mode.
  configure terminal
  c Configure the maximum number of multicast groups allowed for concurrent request globally.
  ip igmp snooping l2-entry-limit *l2-entry-limit*
  The maximum number of multicast groups allowed for concurrent request globally is 64,000 by default.
- Configure the maximum number of multicast groups that can be dynamically learned by a port.
  a Enter the privileged EXEC mode.
  enable
  d Enter the global configuration mode.
  configure terminal
  e Enter the interface configuration mode.
  interface *interface-type interface-number*

f Configure the maximum number of multicast groups that can be dynamically learned by a port.

ip igmp snooping max-groups *max-groups*

The maximum number of multicast groups that can be dynamically learned by a port is 64,000 by default.

1.6.8 Configuring Source Port Check

1. Overview

The source port check function restricts users to receive only multicast traffic on multicast router ports to prevent users from sending invalid multicast traffic.

- After the source port check function is enabled, only multicast traffic received on multicast router ports is valid. Multicast traffic received on other ports is invalid and will be discarded.
- When the source port check function is disabled, multicast traffic received on any port is valid.

2. Restrictions and Guidelines

- To restrict users to receive multicast traffic only on multicast router ports, configure this function.
- If no multicast router port exists after the source port check function is enabled, the device will discard received multicast traffic.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure source port check.

ip igmp snooping source-check port

Source port check is disabled by default.

1.6.9 Configuring Source IP Address Check

1. Overview

The source IP address check function strictly restricts the source IP address of multicast traffic to prevent invalid multicast traffic.

Source IP address check contains the following two configurations:

- Default source IP address check: A source IP address is specified for each multicast group in all VLANs. Only multicast traffic with the source IP address the same as the preset one is valid.
- Group-specific source IP address check: A source IP address is specified for a specific multicast group in a specific VLAN. The multicast device forwards only data traffic of the specific multicast group received in the VLAN that has the same source IP address as the preset one and discards other multicast traffic from the specific multicast group.

2. Restrictions and Guidelines

- When source IP address check is enabled or disabled, all multicast forwarding entries on the L2 device will

be deleted and the device needs to learn entries in the next query interval.

- Group-specific source IP address check can be configured only after default source IP address check is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure default source IP address check.

ip igmp snooping source-check default-server *source-address*

Source IP address check is disabled by default.

(4) Configure group-specific source IP address check.

ip igmp snooping limit-ipmc vlan *vlan-id* **address** *group-address* **server** *source-address*

Only the multicast source address is checked by default.

1.7 Configuring QinQ Processing

1.7.1 Overview

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

- Mode 1: Create multicast entries on the VLAN where the IGMP packets are located. Forwarding IGMP packets on the VLAN where these packets are located is called transparent transmission. For example, IGMP snooping is enabled for a device, Port A on the device is designated as the QinQ port, the default VLAN of this port is VLAN 1, and Port A allows the passage of VLAN 1 and VLAN 10 packets. When an IGMP Report packet is sent from VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 10 and forwards the IGMP Report packet to the multicast router port of VLAN 10.
- Mode 2: Create multicast entries on the default VLAN of the QinQ port. Encapsulate the IGMP packets with the VLAN tag of the default VLAN where the QinQ port is located and forward the packets within the default VLAN. For example, IGMP snooping is enabled for a device, Port A on the device is designated as the QinQ port, the default VLAN of this port is VLAN 1, and Port A allows the passage of VLAN 1 and VLAN 10 packets. When an IGMP Report packet is sent from VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 1, encapsulates the IGMP Report packet with the tag of VLAN 1, and forwards the packet to the multicast router port of VLAN 1.

IGMP snooping works in mode 2 by default. You can run the **ip igmp snooping tunnel** command to enable IGMP snooping to work in mode 1.

1.7.2 Restrictions and Guidelines

If the QinQ port needs to forward multicast packets on the VLANs specified by the VLAN IDs (VIDs) of the packets, transparent packet transmission needs to be configured on the QinQ port.

1.7.3 Prerequisites

- Configuring Basic IGMP Snooping Functions
- Configure basic QinQ functions. For details about QinQ configuration, see "Configuring QinQ" in the *Ethernet Switching Configuration Guide*.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure transparent packet transmission on the QinQ port.

ip igmp snooping tunnel

The function of transparent IGMP packet transmission on the QinQ port is disabled by default.

1.8 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ip igmp snooping statistics	Clears IGMP snooping statistics.
clear ip igmp snooping gda-table	Clears dynamic multicast router ports and member ports.
show ip igmp snooping [**vlan** *vlan-id*]	Displays basic IGMP snooping configurations.
show ip igmp snooping statistics [**vlan** *vlan-id*]	Displays IGMP snooping statistics.
show ip igmp snooping mrouter	Displays multicast router ports.
show ip igmp snooping gda-table	Displays IGMP snooping forwarding entries.
show ip igmp profile [*profile-number*]	Displays a profile.

Command	Purpose
show ip igmp snooping interfaces [*interface-type interface-number*]	Displays IGMP snooping configurations on a port.
show ip igmp snooping querier [**detail**]	Displays the IGMP snooping querier.
debug igmp-snp	Debugs all IGMP snooping functions.
debug igmp-snp event	Debugs IGMP snooping events.
debug igmp-snp packet	Debugs IGMP snooping packets.
debug igmp-snp msf	Debugs communication between IGMP snooping and Multicast Source Filter (MSF).
debug igmp-snp warning	Debugs IGMP snooping warnings.

1.9 Configuration Examples

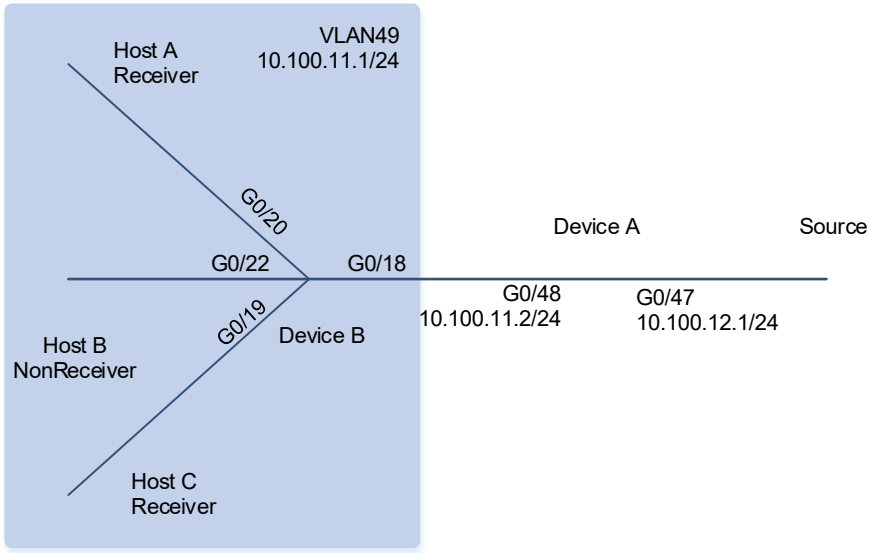
1.9.1 Configuring Basic IGMP Snooping Functions in IVGL Mode

1. Requirements

In the multicast network shown in Figure 1-1, the router (Device A) connects to the user network through the switch (Device B), and IGMP snooping is run on Device A. The multicast source sends data to multicast group 225.0.0.10. There are three hosts (Host A, Host B, and Host C) in the network. Host A and Host C join multicast group 225.0.0.10. Only Host A and Host C can receive multicast data that the multicast source sends to multicast group 225.0.0.10.

2. Topology

Figure 1-1 Topology of Basic IGMP Snooping Functions in IVGL Mode



3. Notes

Configure basic IGMP snooping functions on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and Protocol Independent Multicast-Sparse Mode (PIM-SM) related functions on Device A.
- Enable IGMP snooping and run the IVGL mode on Device B.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# no switchport
DeviceA(config-if-GigabitEthernet 0/48)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
```

```
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 49
DeviceB(config-vlan)# exit
DeviceB(config)# interface vlan 49
DeviceB(config-if-VLAN 49)#ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 49)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

(3) Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl
```

5. Verification

Send packets from the multicast source (10.100.12.2) to multicast group G (225.0.0.10). Enable Host A and Host C to join G.

Run the **show ip igmp snooping gda-table** command on Device B to display the IGMP snooping forwarding entry and check whether the member port list contains only GigabitEthernet 0/19 and GigabitEthernet 0/20.

```
DeviceB> enable
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(DM)
    GigabitEthernet 0/20(DM)

DeviceB#
```

Run the **show ip igmp snooping** command on Device B and check whether the IGMP snooping working mode is IVGL.

```
DeviceB# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 64000
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
IGMP Snooping version: 2
IGMP Preview group aging time: 60(Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)

vlan 49
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
```

```
!
ip multicast-routing
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ip address 10.100.11.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/48
ip pim rp-candidate GigabitEthernet 0/48
!
```

- Device B configuration file

```
hostname DeviceB
!
vlan range 1,49
!
interface GigabitEthernet 0/18
 switchport access vlan 49
!
interface GigabitEthernet 0/19
 switchport access vlan 49
!
interface GigabitEthernet 0/20
 switchport access vlan 49
!
interface GigabitEthernet 0/22
 switchport access vlan 49
!
interface VLAN 49
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
!
ip igmp snooping ivgl
```

```
!
```

7. Common Errors

- The working mode of IGMP snooping is improper.

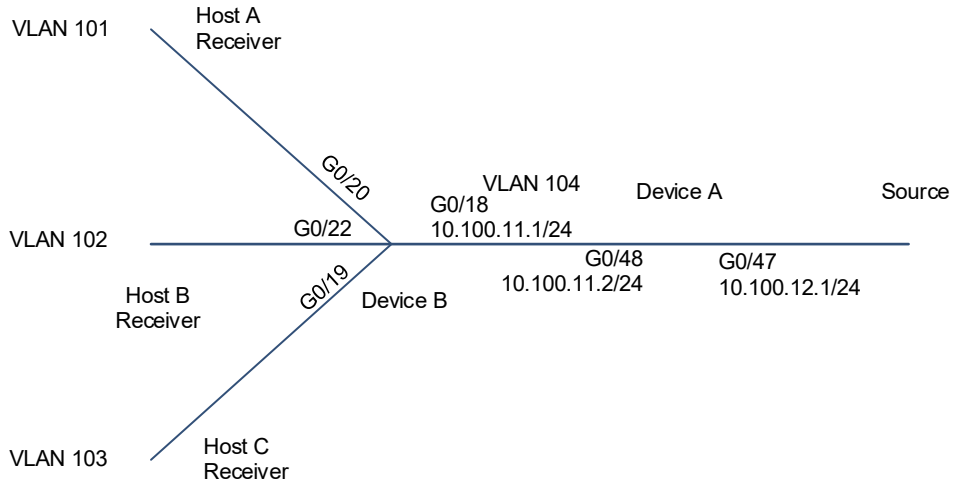
1.9.2 Configuring Basic IGMP Snooping Functions in SVGL Mode

1. Requirements

In the multicast network shown in Figure 1-1, the router (Device A) connects to the user network through the switch (Device B), IGMP snooping is run on Device A, and Device A directly connects to the multicast source. The multicast source sends data to multicast group 225.0.0.10. Host A, Host B, and Host C are connected to VLAN 101, VLAN 102, and VLAN 103, respectively, and the three hosts join multicast group 225.0.0.10. Host A, Host B, and Host C can receive multicast data that the multicast source sends to multicast group 225.0.0.10.

2. Topology

Figure 1-1 Topology of Basic IGMP Snooping Functions in SVGL Mode



3. Notes

Configure basic IGMP snooping functions on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SM related functions on Device A.
- Enable IGMP snooping and run the SVGL mode on Device B.
- Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/48)# switchport trunk native vlan 104
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 101-104
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface VLAN 101
DeviceB(config-if-VLAN 101)# ip address 10.100.101.1 255.255.255.0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ip address 10.100.102.1 255.255.255.0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ip address 10.100.103.1 255.255.255.0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 104)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 104
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
```

```
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 103
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 102
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.101.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.102.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.103.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

(3) Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping svgl
```

(4) Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp profile 1
DeviceB(config-profile)# permit
DeviceB(config-profile)# range 224.1.1.1 238.1.1.1
DeviceB(config-profile)# exit
DeviceB(config)# ip igmp snooping svgl profile 1
DeviceB(config)# ip igmp snooping svgl vlan 104
DeviceB(config)# ip igmp snooping svgl subvlan 101-103
```

5. Verification

Send packets from the multicast source (10.100.12.2) to multicast group G (225.0.0.10). Enable Host A, Host B, and Host C to join G.

Run the **show ip igmp snooping gda-table** command on Device B to display the IGMP snooping forwarding entry and check whether the member port list contains GigabitEthernet 0/19, GigabitEthernet 0/20, and GigabitEthernet 0/22.

```
DeviceB> enable
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

  VLAN(102) 1 OPORTS:
    GigabitEthernet 0/22(D)

  VLAN(103) 1 OPORTS:
    GigabitEthernet 0/19(D)

  VLAN(101) 1 OPORTS:
    GigabitEthernet 0/20(D)

DeviceB#
```

Run the **show ip igmp snooping** command on Device B and check whether the IGMP snooping working mode is SVGL.

```
DeviceB> enable
DeviceB# show ip igmp snooping
IGMP Snooping running mode: SVGL
IGMP Snooping L2-entry-limit: 64000
SVGL vlan: 104
SVGL profile number: 1
IGMP Snooping SVGL subvlan: 101-103
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
IGMP Snooping version: 2
IGMP Preview group aging time: 60(Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
 ip address 10.100.11.2 255.255.255.0
ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/48
ip pim rp-candidate GigabitEthernet 0/48
!
```

- Device B configuration file

```
hostname DeviceB
!
ip igmp profile 1
 permit
 range 224.1.1.1 238.1.1.1
!
vlan range 1,101-104
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 104
!
interface GigabitEthernet 0/19
 switchport access vlan 103
!
```

```
interface GigabitEthernet 0/20
 switchport access vlan 101
!
interface GigabitEthernet 0/22
 switchport access vlan 102
!
interface VLAN 101
 ip address 10.100.101.1 255.255.255.0
!
interface VLAN 102
 ip address 10.100.102.1 255.255.255.0
!
interface VLAN 103
 ip address 10.100.103.1 255.255.255.0
!
interface VLAN 104
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.101.0 0.0.0.255 area 0
 network 10.100.102.0 0.0.0.255 area 0
 network 10.100.103.0 0.0.0.255 area 0
!
ip igmp snooping svgl vlan 104
ip igmp snooping svgl profile 1
ip igmp snooping svgl subvlan 101-103
ip igmp snooping svgl
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The sent multicast traffic is not in the multicast groups associated with the SVGL mode.

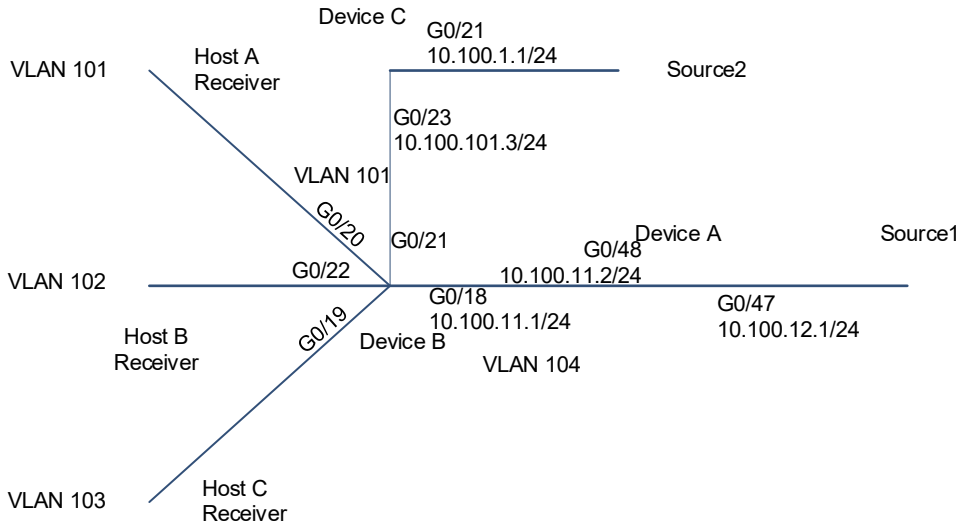
1.9.3 Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

1. Requirements

In the multicast network shown in Figure 1-1, the routers (Device A and Device C) connect to the user network through the switch (Device B), IGMP snooping is run on Device A and Device C, and Device A and Device C directly connect to the multicast sources. Multicast source 1 sends data to multicast group 225.0.0.10, and multicast source 2 sends data to multicast group 239.0.0.11. Host A, Host B, and Host C are connected to VLAN 101, VLAN 102, and VLAN 103, respectively. Host B and Host C join multicast group 225.0.0.10, and Host A joins multicast groups 225.0.0.10 and 239.0.0.11. Host B and Host C can receive multicast data that source 1 sends to multicast group 225.0.0.10, and Host A can receive multicast data that source 1 sends to multicast group 225.0.0.10 and multicast data that source 2 sends to multicast group 239.0.0.11. Host A, Host B, and Host C enjoy shared multicast services, and Host A also enjoys independent multicast services.

2. Topology

Figure 1-1 Topology of Basic IGMP Snooping Functions in IVGL-SVGL Mode



3. Notes

Configure basic IGMP snooping functions in IVGL-SVGL mode on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SM related functions on Device A and Device C.
- Enable IGMP snooping and run the IVGL-SVGL mode on Device B.
- Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/48)# switchport trunk native vlan 104
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 101-104
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface VLAN 101
DeviceB(config-if-VLAN 101)# ip address 10.100.101.1 255.255.255.0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ip address 10.100.102.1 255.255.255.0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ip address 10.100.103.1 255.255.255.0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 104)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 104
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 103
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 101
```

```
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/21
DeviceB(config-if-GigabitEthernet 0/21)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/21)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 102
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.101.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.102.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.103.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

Configure the IP address and unicast routing protocol on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ip address 10.100.1.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# no switchport
DeviceC(config-if-GigabitEthernet 0/23)# ip address 10.100.101.3 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/23)# exit
DeviceC(config)# router ospf 49
DeviceC(config-router)# network 10.100.1.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.101.0 0.0.0.255 area 0
DeviceC(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A and Device C.

Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

Enable multicast routing and PIM-SM related functions on Device C.

```
DeviceC(config)# ip multicast-routing
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ip pim sparse-mode
```

```
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/23)# exit
```

(3) Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl-svgl
```

(4) Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp profile 1
DeviceB(config-profile)# permit
DeviceB(config-profile)# range 224.1.1.1 238.1.1.1
DeviceB(config-profile)# exit
DeviceB(config)# ip igmp snooping svgl profile 1
DeviceB(config)# ip igmp snooping svgl vlan 104
DeviceB(config)# ip igmp snooping svgl subvlan 101-103
```

5. Verification

Run the **show ip igmp snooping gda-table** command on Device B to display the IGMP snooping forwarding entries and check whether the member port list of entry (*, 225.0.0.10, 104) contains GigabitEthernet 0/22, GigabitEthernet 0/20, and GigabitEthernet 0/19 and the member port list of entry (*, 239.0.0.11, 101) contains GigabitEthernet 0/20.

```
DeviceB> enable

DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 239.0.0.11, 101):
  VLAN(101) 2 OPORTS:
    GigabitEthernet 0/20(D)
    GigabitEthernet 0/21(M)

(*, 225.0.0.10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

  VLAN(102) 1 OPORTS:
    GigabitEthernet 0/22(D)

  VLAN(101) 1 OPORTS:
```

```
    GigabitEthernet 0/20(D)

  VLAN(103) 1 OPORTS:
    GigabitEthernet 0/19(D)

DeviceB#
```

Run the **show ip igmp snooping** command on Device B and check whether the IGMP snooping working mode is IVGL-SVGL.

```
DeviceB# show ip igmp snooping
IGMP Snooping running mode: IVGL-SVGL
IGMP Snooping L2-entry-limit: 64000
SVGL vlan: 104
SVGL profile number: 1
IGMP Snooping SVGL subvlan: 101-103
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
IGMP Snooping version: 2
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: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 101
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 102
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
```

```
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 103
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 104
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
 ip address 10.100.11.2 255.255.255.0
ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
```

```
!
ip pim bsr-candidate GigabitEthernet 0/48
ip pim rp-candidate GigabitEthernet 0/48
!
```

- Device B configuration file

```
hostname DeviceB
!
ip igmp profile 1
 permit
 range 224.1.1.1 238.1.1.1
!
vlan range 1,101-104
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 104
!
interface GigabitEthernet 0/19
 switchport access vlan 103
!
interface GigabitEthernet 0/20
 switchport access vlan 101
!
interface GigabitEthernet 0/21
 switchport access vlan 101
!
interface GigabitEthernet 0/22
 switchport access vlan 102
!
interface VLAN 101
 ip address 10.100.101.1 255.255.255.0
!
interface VLAN 102
 ip address 10.100.102.1 255.255.255.0
!
interface VLAN 103
 ip address 10.100.103.1 255.255.255.0
!
interface VLAN 104
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.101.0 0.0.0.255 area 0
 network 10.100.102.0 0.0.0.255 area 0
```

```
 network 10.100.103.0 0.0.0.255 area 0
!
ip igmp snooping svgl vlan 104
ip igmp snooping svgl profile 1
ip igmp snooping svgl subvlan 101-103
ip igmp snooping ivgl-svgl
!
```

- Device C configuration file

```
hostname DeviceC
!
ip multicast-routing
!
interface GigabitEthernet 0/21
 no switchport
 ip address 10.100.1.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ip address 10.100.101.3 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.1.0 0.0.0.255 area 0
 network 10.100.101.0 0.0.0.255 area 0
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The sent multicast traffic is not in the multicast groups associated with the SVGL mode.
- The group addresses of multicast traffic in IVGL mode are within the multicast group range in SVGL mode. As a result, IVGL forwarding cannot be implemented.

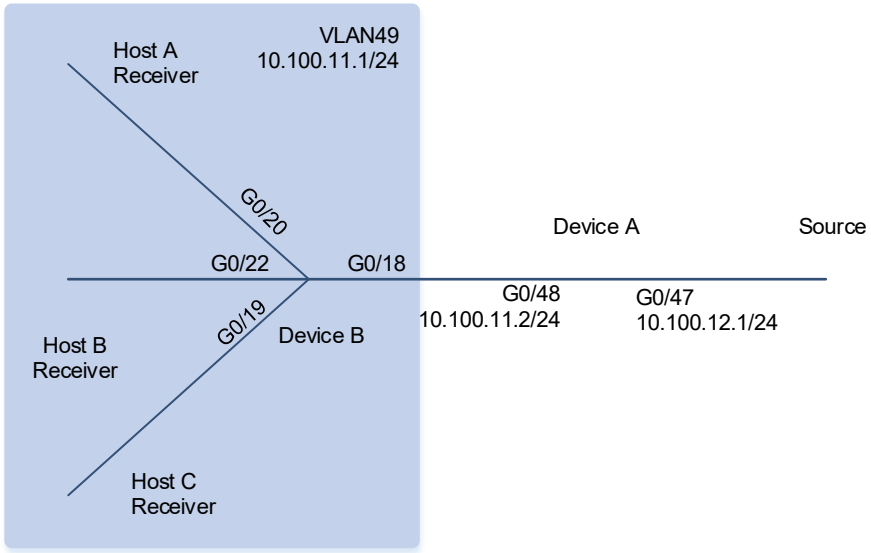
1.9.4 Configuring Static Ports to Implement L2 Multicast

1. Requirements

In the multicast network shown in Figure 1-1, Host A, Host B, and Host C need to receive data that a multicast source sends to a specific multicast group stably. The router (Device A) connects to the user network through the L2 device (Device B). The static IGMP multicast groups 225.0.0.10 to 225.0.0.12 are configured on the user-side L3 port on Device A. Host A and Host B want to receive data of multicast group 225.0.0.10 stably, and Host C wants to receive data of multicast group 225.0.0.11 stably.

2. Topology

Figure 1-1 Topology of Static Ports to Implement L2 Multicast



3. Notes

Configure IGMP snooping static multicast router ports and member ports on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and IGMP static multicast groups on Device A.
- Enable IGMP snooping on Device B.
- Configure static multicast router ports and member ports on Device B.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# no switchport
DeviceA(config-if-GigabitEthernet 0/48)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
```

```
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 49
DeviceB(config-vlan)# exit
DeviceB(config)# interface vlan 49
DeviceB(config-if-VLAN 49)#ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 49)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

(2) Enable IP multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ip igmp static-group 225.0.0.10
DeviceA(config-if-GigabitEthernet 0/48)# ip igmp static-group 225.0.0.11
DeviceA(config-if-GigabitEthernet 0/48)# ip igmp static-group 225.0.0.12
DeviceA(config-if-GigabitEthernet 0/48)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

(3) Enable basic IGMP snooping functions on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl
```

(4) Configure static multicast router ports and member ports on Device B.

```
DeviceB> enable
```

```
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping vlan 49 static 225.0.0.11 interface
GigabitEthernet 0/19
DeviceB(config)# ip igmp snooping vlan 49 static 225.0.0.10 interface
GigabitEthernet 0/22
DeviceB(config)# ip igmp snooping vlan 49 static 225.0.0.10 interface
GigabitEthernet 0/20
DeviceB(config)# ip igmp snooping vlan 49 mrouter interface GigabitEthernet
0/18
```

5. Verification

Run the **show ip igmp snooping mrouter** command and check whether the static router port is GigabitEthernet 0/18.

```
DeviceB> enable
DeviceB# show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 49):
  VLAN(49)  1 MROUTES:
    GigabitEthernet 0/18(DS)

(*, *, 101):
  VLAN(101)  1 MROUTES:
    GigabitEthernet 0/21(D)

DeviceB#
```

Run the **show ip igmp snooping gda-table** command and check whether the static member ports of multicast group 225.0.0.10 are GigabitEthernet 0/20 and GigabitEthernet 0/22 and the static member port of multicast group 225.0.0.11 is GigabitEthernet 0/19.

```
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/20(S)
    GigabitEthernet 0/22(S)

(*, 225.0.0.11, 49):
  VLAN(49) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(S)
```

```
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ip address 10.100.11.2 255.255.255.0
 ip igmp static-group 225.0.0.10
 ip igmp static-group 225.0.0.11
 ip igmp static-group 225.0.0.12
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/47
ip pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
vlan range 1,49
!
interface GigabitEthernet 0/18
 switchport access vlan 49
!
interface GigabitEthernet 0/19
 switchport access vlan 49
!
interface GigabitEthernet 0/20
 switchport access vlan 49
!
interface GigabitEthernet 0/22
```

```
 switchport access vlan 49
!
interface VLAN 49
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
!
ip igmp snooping ivgl
!
ip igmp snooping vlan 49 static 225.0.0.11 interface GigabitEthernet 0/19
ip igmp snooping vlan 49 static 225.0.0.10 interface GigabitEthernet 0/22
ip igmp snooping vlan 49 static 225.0.0.10 interface GigabitEthernet 0/20
ip igmp snooping vlan 49 mrouter interface GigabitEthernet 0/18
!
```

7. Common Errors

- Basic IGMP snooping functions are not configured or fail to be configured.

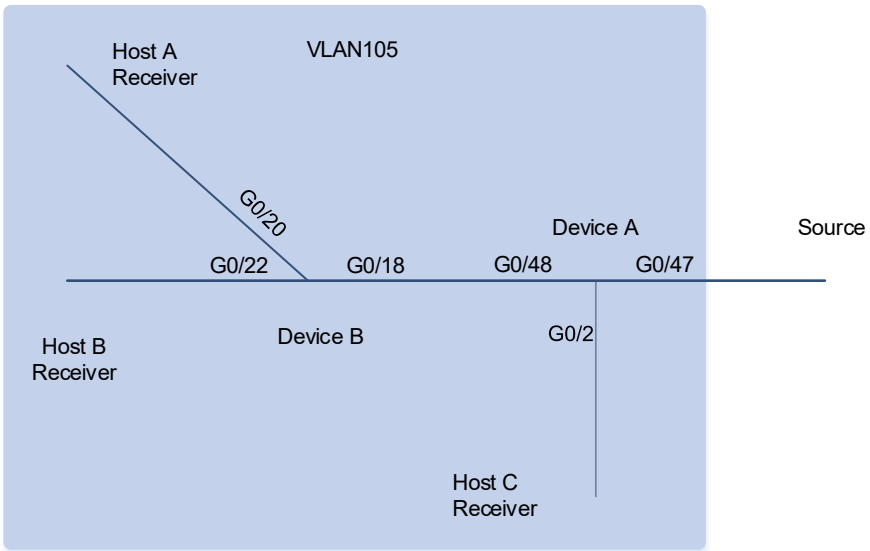
1.9.5 Configuring IGMP Snooping Querier

1. Requirements

In a two-layer multicast network, as shown in Figure 1-1, the multicast source sends multicast data to multicast groups 225.0.0.10 and 225.0.0.11. Host A and Host C join multicast group 225.0.0.10, and Host B joins multicast group 225.0.0.11. All receivers use IGMPv2. IGMP snooping is used to transfer multicast data in the two-layer network.

2. Topology

Figure 1-1 Topology of IGMP Snooping Querier



3. Notes

Enable IGMP snooping on Device A and Device B, and configure Device A as the IGMP snooping querier.

- Configure VLANs and IP addresses on Device A and Device B.
- Enable IGMP snooping and run the IVGL mode on Device A and Device B.
- Configure the IGMP snooping querier function for VLAN 105 on Device A.

4. Procedure

(1) Configure VLANs and IP addresses on Device A and Device B.

Configure the VLAN and IP address on Device A.

```
DeviceA>enable
DeviceA# configure terminal
DeviceA(config)# vlan range 1,105
DeviceA(config)# interface VLAN105
DeviceA(config-if-VLAN105)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-VLAN105)# exit
DeviceA(config)# interface GigabitEthernet0/47
DeviceA(config-if-GigabitEthernet0/47)# switchport access vlan 105
DeviceA(config-if-GigabitEthernet0/47)# interface GigabitEthernet0/48
DeviceA(config-if-GigabitEthernet0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet0/48)# switchport trunk native vlan 105
DeviceA(config-if-GigabitEthernet0/48)# exit
```

Configure the VLAN and IP address on Device B.

```
DeviceB>enable
DeviceB# configure terminal
DeviceB(config)# vlan range 1,105
DeviceB(config)# interface VLAN105
DeviceB(config-if-VLAN105)# ip address 10.100.12.3 255.255.255.0
DeviceB(config-if-VLAN105)# exit
DeviceB(config-if-GigabitEthernet 0/18)# interface GigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/2)# exit
DeviceB(config)#interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 105
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 105
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 105
DeviceB(config-if-GigabitEthernet 0/22)# exit
```

(2) Configure basic IGMP snooping functions and run the IVGL mode on Device A and Device B.

Enable IGMP snooping and run the IVGL mode on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip igmp snooping ivgl
```

Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl
```

(3) Configure the IGMP snooping querier function on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)#ip igmp snooping querier
DeviceA(config)#ip igmp snooping querier address 10.100.12.1
DeviceA(config)#ip igmp snooping vlan 105 querier
```

5. Verification

Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.

```
DeviceA> enable
DeviceA# show ip igmp snooping querier
Vlan      IP Address           IGMP Version           Port
-----------------------------------------------------------
105       10.100.12.1             2                   switch
DeviceA#
DeviceA# show ip igmp snooping querier vlan 105

Vlan 105:   IGMP switch querier status
-----------------------------------------------------------
elected querier is 10.100.12.1         (this switch querier)
-----------------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 10.100.12.1
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 125
operational state              : Querier
operational version            : 2
DeviceA#
```

Run the **show ip igmp snooping gda-table** command on Device A and check whether the outbound ports of multicast group 225.0.0.10 are GigabitEthernet0/2 and GigabitEthernet0/48 and the outbound port of multicast group 225.0.0.11 is GigabitEthernet0/48.

```
DeviceA> enable
DeviceA# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
```

```
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 105):
  VLAN(105) 2 OPORTS:
    GigabitEthernet0/2(D)
    GigabitEthernet0/48(D)

(*, 225.0.0.11, 105):
  VLAN(105) 1 OPORTS:
    GigabitEthernet0/48(D)

DeviceA#
```

Run the **show ip igmp snooping gda-table** command on Device B and check whether the outbound port of multicast group 225.0.0.10 is GigabitEthernet0/20 and the outbound port of multicast group 225.0.0.11 is GigabitEthernet0/22.

```
DeviceB> enable
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 105):
  VLAN(105) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/20(D)

(*, 225.0.0.11, 105):
  VLAN(105) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/22(D)

DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
vlan range 1,105
!
interface GigabitEthernet0/2
 switchport access vlan 105
!
interface GigabitEthernet0/47
 switchport access vlan 105
!
```

```
interface GigabitEthernet0/48
 switchport mode trunk
 switchport trunk native vlan 105
!
interface VLAN105
 ip address 10.100.12.1 255.255.255.0
!
ip igmp snooping ivgl
ip igmp snooping querier
ip igmp snooping querier address 10.100.12.1
ip igmp snooping vlan 105 querier
!
```

- Device B configuration file

```
hostname DeviceA
!
vlan range 1,105
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 105
!
interface GigabitEthernet 0/20
 description cyx
 switchport access vlan 105
!
interface GigabitEthernet 0/22
 description cyx
 switchport access vlan 105
!
interface VLAN 105
 ip address 10.100.12.3 255.255.255.0
!
ip igmp snooping ivgl
!
```

7. Common Errors

- The source IP address of Query packets sent by the querier is not configured. As a result, the querier function does not take effect.