Contents

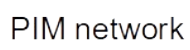
1 Configuring MLD Snooping

1.1 Introduction

Multicast Listener Discovery (MLD) snooping is a process of snooping protocol packets between an L3 multicast device and hosts to manage and control forwarding of IPv6 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 MLD snooping function is configured, the L2 switch can listen to MLD 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

MLD 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 MLD 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 MLD snooping is not configured on the L2 device, IPv6 multicast packets are broadcast in the VLAN. As shown in Figure 1-2, when MLD snooping is enabled on the L2 device, IPv6 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 MLD Snooping Is Disabled

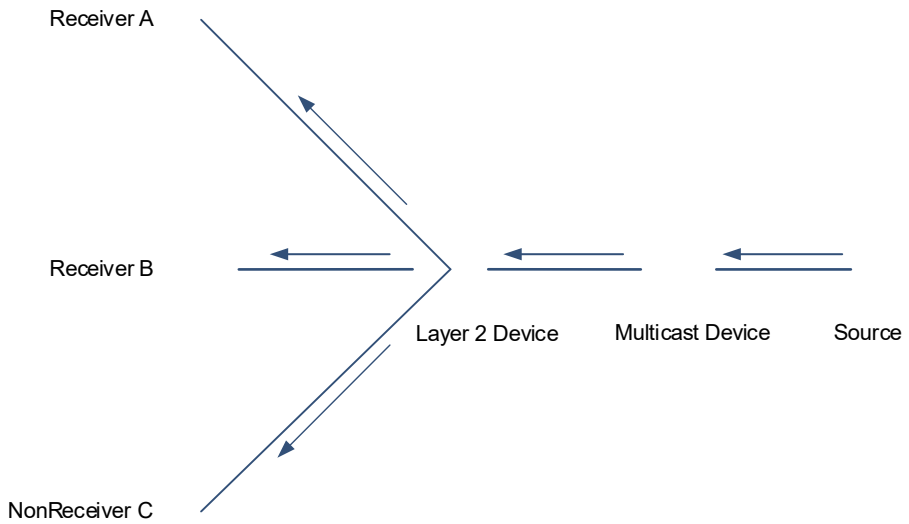
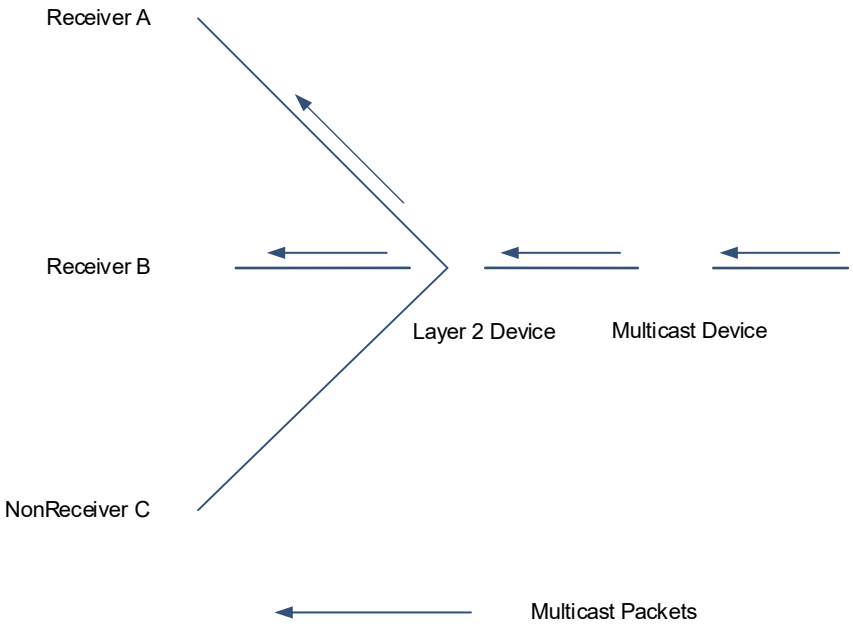


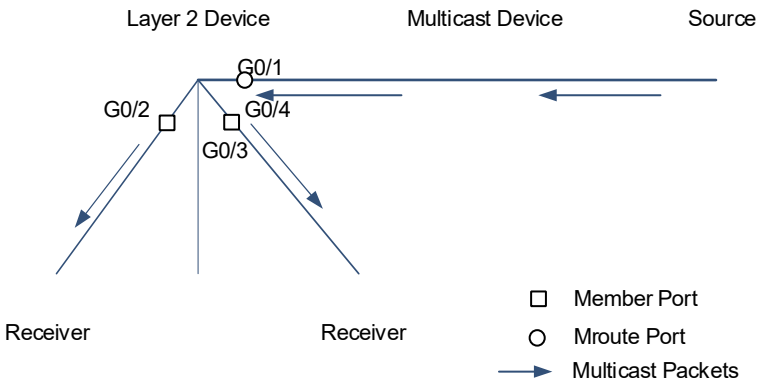
Figure 1-2 Multicast Data Transmission When MLD Snooping Is Enabled



1.1.3 Port Types

MLD snooping is enabled on a per-VLAN basis. MLD snooping ports are ports in a VLAN. The device running MLD 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 MLD 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 MLD 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 MLD 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, MLD 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 MLD snooping analyzes received MLD packets to discover and identify multicast router ports and member ports and establish and maintain MLD snooping forwarding entries. The device can identify and process the following types of MLD packets:

1. Query Packets

An L3 multicast device regularly sends an MLD general Query packet to all hosts and other multicast devices (with the address of FF02::1) in the local network segment to query the IPv6 multicast group members in this network segment. When receiving the MLD general Query packet, a multicast device forwards the packet through all ports in the VLAN except the one receiving the packet and processes the port receiving the packet as follows:

- Reset the aging timer of the port if the port is in the multicast router port list.
- Add the port to the multicast router port list if the port is not in the multicast router port list and start the aging timer of the port.
- When the L2 multicast device receives an MLD group-specific Query packet, it does not update the preceding timers.

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.

When receiving a Report packet, the device running MLD snooping forwards it to all multicast router ports in the VLAN, retrieves the address of the IPv6 multicast group that the host needs to join from the packet, and processes the port receiving the packet as follows:

- The device creates a forwarding entry for the IPv6 multicast group if no forwarding entry for the IPv6 multicast group exists, adds the port to the outbound port list as a dynamic member port, and starts the aging timer of the port.
- The device adds the port to the outbound port list as a dynamic member port and starts its aging timer if the forwarding entry of the IPv6 multicast group exists but the port is not contained in the outbound port list.
- The device resets the aging timer of the port if the forwarding entry of the IPv6 multicast group exists and the port is contained in the outbound port list.

3. Leave Packets

When a host leaves an IPv6 multicast group, it sends an MLD Leave packet (with the address of FF02::2) to notify the multicast device. When receiving a Leave packet, the device running MLD snooping 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 MLD 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 MLD 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

MLD snooping configuration includes the following tasks:

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

- Configuring Basic MLD Snooping Functions in IVGL Mode
- Configuring Basic MLD Snooping Functions in SVGL Mode
- Configuring Basic MLD 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
- Configuring the Maximum Response Time for Query Packets

(3) All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring Multicast Group Filtering on a Port
- Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port
- Configuring Source Port Check

1.3 Configuring Basic MLD Snooping Functions

1.3.1 Overview

The device running MLD snooping can provide independent or shared multicast services for user VLANs when operating 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 IPv6 multicast function are mutually exclusive. If the IPv6 multicast function needs to be enabled on the device running MLD snooping, the device can operate only in IVGL mode.
- If the device running MLD snooping operates in SVGL or IVGL-SVGL mode, a profile must be defined to specify the multicast groups associated with the SVGL mode.

1.3.3 Configuration Tasks

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

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

1.3.4 Configuring Basic MLD Snooping Functions in IVGL Mode

1. Overview

In IVGL mode, the device running MLD 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 MLD snooping globally on all L2 access devices connecting to hosts.
- After MLD snooping is enabled globally, it takes effect to all VLANs. You can disable MLD 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 the IPv6 MLD snooping function and run the IVGL mode.

ipv6 mld snooping ivgl

MLD snooping is disabled by default.

(4) (Optional) Disable MLD snooping on a specified VLAN.

no ipv6 mld snooping vlan *vlan-id*

After MLD snooping is enabled globally, it takes effect to all VLANs by default. If MLD snooping is disabled globally, it is ineffective on all VLANs.

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

1.3.5 Configuring Basic MLD Snooping Functions in SVGL Mode

1. Overview

In SVGL mode, the device running MLD 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

- Multicast services can be shared among VLANs. After configuring the SVGL mode, you need to configure multicast groups applied in 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 1.5.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 MLD snooping function and run the SVGL mode.

ipv6 mld snooping svgl

MLD snooping is disabled by default.

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

ipv6 mld snooping svgl profile *profile-number*

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

(5) (Optional) Specify a shared VLAN.

ipv6 mld snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

1.3.6 Configuring Basic MLD 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 MLD 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 1.5.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 MLD snooping function and run the IVGL-SVGL mode.

ipv6 mld snooping ivgl-svgl

MLD snooping is disabled by default.

(4) (Optional) Specify a shared VLAN.

ipv6 mld snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

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 MLD snooping membership quickly.

1.4.2 Restrictions and Guidelines

Configuring Basic MLD Snooping Functions Related configuration functions take effect only after basic MLD 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
- Configuring the Maximum Response Time for Query Packets

1.4.4 Configuring a Static Multicast Router Port

1. Overview

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

ipv6 mld 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.

ipv6 mld snooping vlan *vlan-id* **static** *ipv6-group-address* **interface** *interface-type interface-number*

No static member port is configured by default.

1.4.6 Configuring Report Packet Suppression

1. Overview

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

When Report packet suppression is configured, the MLD multicast device forwards only 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 helps reduce the number of packets in the network.

2. Restrictions and Guidelines

Only MLDv1 Report packets can be suppressed, and MLDv2 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.

ipv6 mld 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 MLDv1 Leave packet and MLDv2 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.

ipv6 mld snooping fast-leave enable

The port fast leave function is disabled by default.

1.4.8 Configuring Dynamic Multicast Router Port Learning

1. Overview

In some test scenarios, a user host may send Query packets and PIMv6 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 PIMv6 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.

ipv6 mld snooping [**vlan** *vlan-id*] **mrouter learn**

Dynamic multicast router port learning is enabled by default.

1.4.9 Configuring the Aging Time for Dynamic Multicast Router Ports

1. Overview

A multicast router port is used to receive uplink multicast data and forward MLD Report and Leave packets. After enabling MLD 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.

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.

ipv6 mld snooping dyn-mr-aging-time *dynamic-mroute-aging-time*

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

1.4.10 Configuring the Aging Time for Dynamic Member Ports

1. Overview

When the device running MLD snooping receives an MLD 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. If 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 MLD 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 this command is configured, the aging timer value of dynamic member ports is *host-aging-time* for subsequent MLD Join packets. The aging time takes effect immediately after configuration and the started member port timers are 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.

ipv6 mld snooping host-aging-time *host-aging-time*

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

1.4.11 Configuring the Maximum Response Time for Query Packets

1. Overview

When hosts in the directly-connected network segment of the device serving as the MLD 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

- When receiving an MLD general Query packet, the multicast device will update the aging timers of all member ports. The timer time is the maximum response time for Query packets. After the timer expires, the device regards that no group member receives multicast traffic through a port and deletes the port from the MLD snooping forwarding table.
- When receiving an MLD group-specific Query packet, the multicast device will start the aging timers of all member ports of the specific group. The timer time is the maximum response time for Query packets. After the timer expires, the device regards that no group member receives multicast traffic through a port and deletes the port from the MLD snooping forwarding table.
- For MLDv2 group-specific Query packets, the multicast device does not update the timers.
- The configured response time for Query packets takes effect when the next Query packet is received.

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.

ipv6 mld snooping query-max-response-time *query-max-response-time*

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

1.5 Configuring Multicast Security Control

1.5.1 Overview

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

1.5.2 Prerequisites

Configuring Basic MLD Snooping Functions

1.5.3 Configuration Tasks

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

- Configuring a Profile
- Configuring Multicast Group Filtering on a Port
- Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port
- Configuring Source Port Check

1.5.4 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.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a profile.

ipv6 mld profile *profile-number*

No profile is created by default.

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

range *low-ipv6-address* [*high-ipv6-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.

- 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.

1.5.5 Configuring Multicast Group Filtering on a Port

1. Overview

Generally, the device running ports 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 port, you can restrict the multicast groups that users can join on the port.

3. Prerequisites

Before configuring a range of multicast groups for a profile, 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 1.5.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure multicast group filtering on a port.

ipv6 mld snooping filter *profile-number*

The multicast group filtering function is disabled on a port by default.

1.5.6 Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port

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 on a port.

2. Restrictions and Guidelines

Only dynamically learned multicast groups on a port are counted. Statically configured multicast groups are excluded.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

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

ipv6 mld snooping max-groups *max-groups-number*

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

1.5.7 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.

ipv6 mld snooping source-check port

Source port check is disabled by default.

1.6 Monitoring

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

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 ipv6 mld snooping gda-table	Clears MLD snooping multicast forwarding entries.
clear ipv6 mld snooping statistics	Clears MLD snooping statistics.
show ipv6 mld snooping	Displays the current MLD snooping mode.
show ipv6 mld snooping gda-table	Displays MLD snooping forwarding entries.
show ipv6 mld snooping statistics	Displays MLD snooping statistics.
show ipv6 mld snooping mrouter	Displays MLD snooping multicast router ports.
show ipv6 mld snooping interfaces [*interface-type interface-name*]	Displays MLD snooping interface information, interface filtering profile, and maximum number of multicast groups that can be dynamically learned by a port.
show ipv6 mld snooping vlan *vlan-id*	Displays multicast information about a single VLAN, on which MLD snooping is configured.
show ipv6 mld profile *profile-number*	Displays an MLD profile.

1.7 Configuration Examples

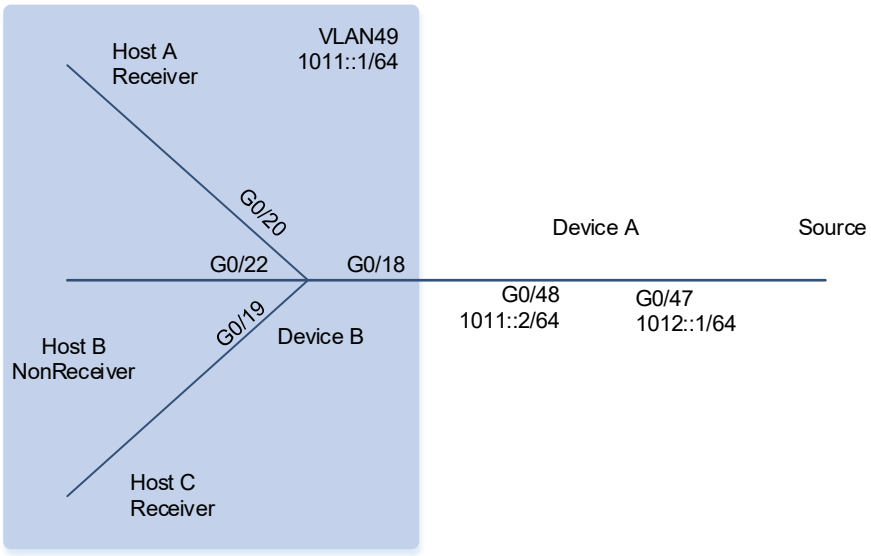
1.7.1 Configuring Basic MLD Snooping Functions in IVGL Mode

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 MLD snooping is run on Device A. The multicast source sends data to multicast group FF14::10. There are three hosts (Host A, Host B, and Host C) in the network. Host A and Host C join multicast group FF14::10. Only Host A and Host B can receive multicast data that the multicast source sends to multicast group FF14::10.

2. Topology

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



3. Notes

Configure basic MLD snooping functions on Device B.

- Configure the IPv6 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-SMv6 related functions on Device A.
- Enable MLD snooping and run the IVGL mode on Device B.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IPv6 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)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 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)# ipv6 address 1011::2/64
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/48)# exit
```

```
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 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)# ipv6 address 1011::1/64
DeviceB(config-if-VLAN 49)# ipv6 ospf 4949 area 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)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

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

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping ivgl
```

5. Verification

Send packets from the multicast source (1012::2) to multicast group G (FF14::10). Enable Host A and Host C to join G.

Run the **show ipv6 mld snooping gda-table** command on Device B to display the MLD snooping forwarding entry and check whether the member port list contains only GigabitEthernet 0/19 and GigabitEthernet 0/20.

```
DeviceB> enable
DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF14::10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(M)
    GigabitEthernet 0/20(DM)

DeviceB#
```

Run the **show ipv6 mld snooping** command on Device B and check whether the MLD snooping working mode is IVGL.

```
DeviceB# show ipv6 mld snooping
MLD-snooping mode: IVGL
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
MLD Snooping version: 1
MLD Tunnel: Disable

vlan 49
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/47
 no switchport
```

```
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 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
 ipv6 address 1011::1/64
 ipv6 ospf 4949 area 0
!
Ipv6 mld snooping ivgl
!
```

7. Common Errors

- The working mode of MLD snooping is improper.

1.7.2 Configuring Basic MLD Snooping Functions in SVGL Mode

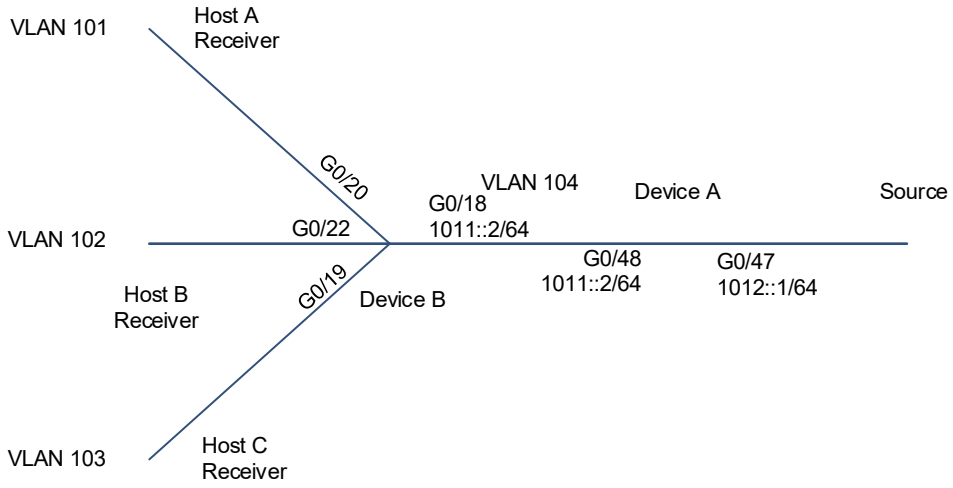
1. Requirements

In the multicast network shown in Figure 1-1, the router (Device A) connects to the user network through the switch (Device B), MLD snooping is run on Device A, and Device A directly connects to the multicast source. The multicast source sends data to multicast group FF14::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 FF14::10. Host A, Host B, and Host C can receive multicast data that the multicast source sends to multicast group FF14::10.

2. Topology

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



3. Notes

Configure basic MLD snooping functions on Device B.

- Configure the IPv6 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-SMv6 related functions on Device A.
- Enable MLD snooping and run the SVGL mode on Device B.
- Configure the multicast groups associated with the MLD snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IPv6 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)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 address 1011::2/64
```

```
DeviceA(config-if-VLAN 104)# ipv6 ospf 4949 area 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)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 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)# ipv6 address 1010::1/64
DeviceB(config-if-VLAN 101)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ipv6 address 1020::1/64
DeviceB(config-if-VLAN 102)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ipv6 address 1030::1/64
DeviceB(config-if-VLAN 103)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceB(config-if-VLAN 104)# ipv6 ospf 4949 area 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)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

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

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

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

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping svgl
```

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

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld profile 1
DeviceB(config-profile)# permit
DeviceB(config-profile)# range ff13::1 ff14::fff
DeviceB(config-profile)# exit
DeviceB(config)# ipv6 mld snooping svgl profile 1
DeviceB(config)# ipv6 mld snooping svgl vlan 104
```

5. Verification

Send packets from the multicast source (1012::2) to multicast group G (FF14::10). Enable Host A, Host B, and Host C to join G.

Run the **show ipv6 mld snooping gda-table** command on Device B to display the MLD 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 ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF14::10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

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

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

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

DeviceB#
```

Run the **show ipv6 mld snooping** command on Device B and check whether the MLD snooping working mode is SVGL.

```
DeviceB> enable
DeviceB# show ipv6 mld snooping
MLD-snooping mode: SVGL
SVGL vlan: 104
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
MLD Snooping version: 1
MLD Tunnel: Disable
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode!
!
ipv6 router ospf 4949
```

```
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 mld profile 1
 permit
 range FF13::1 FF14::FFF
!
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
 ipv6 address 1010::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 102
 ipv6 address 1020::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 103
 ipv6 address 1030::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 104
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
!
ipv6 router ospf 4949
 graceful-restart
!
```

```
ipv6 mld snooping svgl vlan 104
ipv6 mld snooping svgl profile 1
ipv6 mld snooping svgl
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The address of the sent multicast traffic is not within the range of multicast groups associated with the SVGL mode.

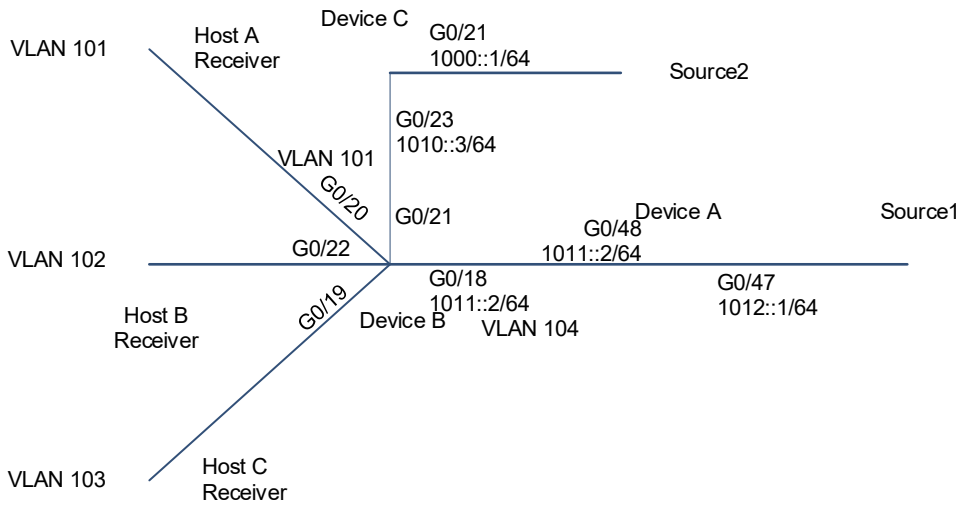
1.7.3 Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode

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), MLD 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 FF14::10, and multicast source 2 sends data to multicast group FF15::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 FF14::10, and Host A joins multicast groups FF14::10 and FF15::11. Host B and Host C can receive multicast data that source 1 sends to multicast group FF14::10, and Host A can receive multicast data that source 1 sends to multicast group FF14::10 and multicast data that source 2 sends to multicast group FF15::11. Host A, Host B, and Host C enjoy shared multicast services, and Host A also enjoy independent multicast services.

2. Topology

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



3. Notes

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

- Configure the IPv6 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-SMv6 related functions on Device A and Device C.
- Enable MLD snooping and run the IVGL-SVGL mode on Device B.
- Configure the multicast groups associated with the MLD snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IPv6 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)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceA(config-if-VLAN 104)# ipv6 ospf 4949 area 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)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 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)# ipv6 address 1010::1/64
DeviceB(config-if-VLAN 101)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ipv6 address 1020::1/64
DeviceB(config-if-VLAN 102)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ipv6 address 1030::1/64
DeviceB(config-if-VLAN 103)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
```

```
DeviceB(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceB(config-if-VLAN 104)# ipv6 ospf 4949 area 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)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

Configure the IPv6 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)# ipv6 address 1000::1/64
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 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)# ipv6 address 1010::3/64
DeviceC(config-if-GigabitEthernet 0/23)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/23)# exit
DeviceC(config)# ipv6 router ospf 4949
DeviceC(config-router)# exit
```

(2) Enable IPv6 multicast routing and PIM-SMv6 related functions on Device A and Device C.

Enable IPv6 multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
```

```
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

Enable multicast routing and PIM-SMv6 related functions on Device C.

```
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/23)# exit
```

(3) Enable MLD snooping and run the IVGL-SVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping ivgl-svgl
```

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

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld profile 1
DeviceB(config-profile)# permit
DeviceB(config-profile)# range ff13::1 ff14::fff
DeviceB(config-profile)# exit
DeviceB(config)# ipv6 mld snooping svgl profile 1
DeviceB(config)# ipv6 mld snooping svgl vlan 104
```

5. Verification

Run the **show ipv6 mld snooping gda-table** command on Device B to display the MLD snooping forwarding entries and check whether the member port list of entry (*, FF14::10, 104) contains GigabitEthernet 0/22, GigabitEthernet 0/20, and GigabitEthernet 0/19 and the member port list of entry (*, FF15::11, 101) contains GigabitEthernet 0/20.

```
DeviceB> enable

DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF15::11, 101):
  VLAN(101) 2 OPORTS:
    GigabitEthernet 0/20(D)
    GigabitEthernet 0/21(M)

(*, FF14::10, 104):
```

```
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

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

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

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

DeviceB#
```

Run the **show ipv6 mld snooping** command on Device B and check whether the MLD snooping working mode is IVGL-SVGL.

```
DeviceB# show ipv6 mld snooping
MLD-snooping mode: IVGL-SVGL
SVGL vlan: 104
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
MLD Snooping version: 1
MLD Tunnel: Disable

vlan 1
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 101
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 102
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
```

```
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 103
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 104
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

```
Device A configuration file
hostname DeviceA
!
ipv6 multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode!
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 mld profile 1
 permit
 range FF13::1 FF14::FFF
!
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
 ipv6 address 1010::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 102
 ipv6 address 1020::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 103
 ipv6 address 1030::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 104
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 mld snooping svgl vlan 104
ipv6 mld snooping svgl profile 1
```

```
ipv6 mld snooping ivgl-svgl
!
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 1000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ipv6 address 1010::3/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The address of sent multicast traffic is not within the range of multicast groups associated with the SVGL mode.
- The multicast 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.

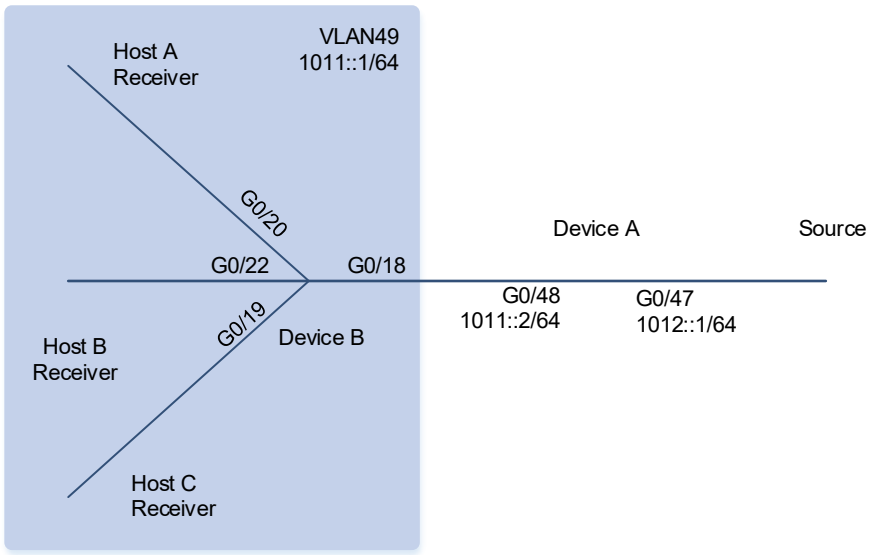
1.7.4 Configuring Static Ports to Implement L2 Multicast

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 MLD multicast groups FF14::10 to FF14::12 are configured on the user-side L3 port on Device A. Host A and Host B want to receive data of multicast group FF14::10 stably, and Host C wants to receive data of multicast group FF14::11.

2. Topology

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



3. Notes

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

- Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and MLD static multicast groups on Device A.
- Enable MLD snooping on Device B.
- Configure static multicast router ports and member ports on Device B.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IPv6 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)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 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)# ipv6 address 1011::2/64
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/48)# exit
```

```
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 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)# ipv6 address 1011::1/64
DeviceB(config-if-VLAN 49)# ipv6 ospf 4949 area 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)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

(2) Enable IPv6 multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 mld static-group ff14::10
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 mld static-group ff14::11
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 mld static-group ff14::12
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

(3) Enable MLD snooping functions on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping ivgl
```

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

```
DeviceB> enable
```

```
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping vlan 49 static ff14::11 interface
GigabitEthernet 0/19
DeviceB(config)# ipv6 mld snooping vlan 49 static ff14::10 interface
GigabitEthernet 0/22
DeviceB(config)# ipv6 mld snooping vlan 49 static ff14::10 interface
GigabitEthernet 0/20
DeviceB(config)# ipv6 mld snooping vlan 49 mrouter interface GigabitEthernet
0/18
```

5. Verification

Run the **show ipv6 mld snooping mrouter** command and check whether the static router port is GigabitEthernet 0/18.

```
DeviceB> enable
DeviceB# show ipv6 mld 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 ipv6 mld snooping gda-table** command and check whether the static member ports of multicast group FF14::10 are GigabitEthernet 0/20 and GigabitEthernet 0/22 and the static member port of multicast group FF14::11 is GigabitEthernet 0/19.

```
DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF14::10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/20(S)
    GigabitEthernet 0/22(S)

(*, FF14::11, 49):
  VLAN(49) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(S)
```

```
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet0/48
 no switchport
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 mld static-group ff14::10
 ipv6 mld static-group ff14::11
 ipv6 mld static-group ff14::12
 ipv6 pim sparse-mode
!
Ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 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
 ipv6 address 1011::1/64
 ipv6 ospf 4949 area 0
!
router ospf 49
 graceful-restart
!
ipv6 mld snooping ivgl
!
ipv6 mld snooping vlan 49 static FF14::11 interface GigabitEthernet 0/19
ipv6 mld snooping vlan 49 static FF14::10 interface GigabitEthernet 0/22
ipv6 mld snooping vlan 49 static FF14::10 interface GigabitEthernet 0/20
ipv6 mld snooping vlan 49 mrouter interface GigabitEthernet 0/18
!
```

7. Common Errors

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