Multicast Configuration, Cisco Catalyst PON Series Switches

First Published: 2020-11-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Configuring Multicast in the GPON Network** 1

Information About Configuring Multicast in the GPON Network 1

About Multicast 1

About IGMP Snooping 1

About Multicast Group Entry 1

About Multicast Group Learning Limitation 2

About Fast Leave 2

About VLAN tagging on Downlink Multicast Packets 2

How to Configure Multicast in the GPON Network 2

Configuring IGMP Snooping 2

Configuring Multicast Group Learning Limitation 3

Configuring Fast Leave 4

Configuring Downlink Multicast Packet Tagging Rule 5

Monitoring Multicast Entry 6

Configuration Examples for Multicast in the GPON Network 7

Example: Configuring IGMP 7

CHAPTER 2 **Configuring IGMP Snooping** 9

Information About IGMP Snooping 9

How to Configure SNMP Snooping 10

Enabling IGMP Snooping 10

Configuring the IGMP Snooping Timer 11

Configuring Fast Leave 12

Configuring the Maximum Number of Multicast Groups 12

Configuring the IGMP-Snooping Learning Strategy 14

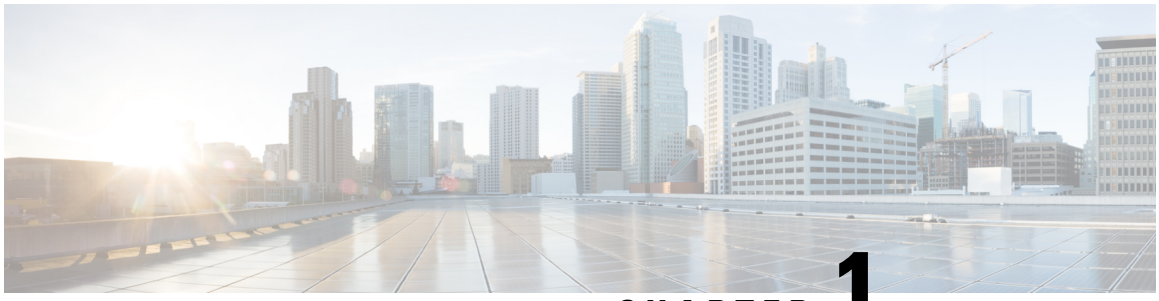
Configuring the IGMP Snooping Querier 15

Configuring the Route Port 16
Configuring a Multicast VLAN for Internet Group Management Protocol Packets 17
Configuring a Port to Record the Host MAC Address 18
Configuring the Suppression of a Multicast Report 18
Configuring the Dropping of Query and Report Packets 19
Configuring the IGMP Snooping Blocked List and Allowed List Profiles 20
Verifying IGMP Snooping Configuration 21
Configuration Examples for IGMP Snooping 22
Example: Enabling IGMP Snooping 22
Example: Displaying the Multicast Group Learnt by a Device 22

CHAPTER 3 **Configuring MLD Snooping** 23
Information About MLD Snooping 23
How to Configure MLD Snooping 23
Enabling MLD Snooping 23
Configuring MLD Snooping Timer 24
Configuring Fast-Leave 24
Configuring Maximum Multicast Groups on a Port 25
Configuring Multicast Learning Strategy of MLD Snooping 26
Configuring MLD Snooping Querier 26
Configuring a Routing Port 28
Configuring a Multicast VLAN 28
Configuring a Port to Record Host MAC Address 29
Verifying MLD Snooping Configuration 29
Configuration Example for MLD Snooping 30

CHAPTER 4 **Configuring Static Multicast Tables** 33
Information About Static Multicast Tables 33
How to Configure Static Multicast Tables 33
Configuring a Static Multicast Group 33
Adding a Port to a Static Multicast Group 34
Configuring a Proxy Port 34
Configuration Examples for Static Multicast Tables 35
Example: Creating a Static Multicast Group 35

Example: Adding a Port to a Static Multicast Group 35



CHAPTER 1

Configuring Multicast in the GPON Network

- Information About Configuring Multicast in the GPON Network, on page 1
- How to Configure Multicast in the GPON Network, on page 2
- Configuration Examples for Multicast in the GPON Network, on page 7

Information About Configuring Multicast in the GPON Network

About Multicast

The GPON system works on a master-slave ONU Management Control Interface (OMCI) protocol. In the GPON system, the OLT is the master, the ONT is the slave and the OMCI protocol allows the OLT to configure, manage and control the attached ONT device. The OMCI protocol establishes a proprietary OMCI channel transmission control messages between the OLT and the ONT. The configuration of the ONT-related multicast function is configured and delivered through the OLT. There are two types of ONT multicast modes:

- IGMP-snooping mode
- Controllable multicast mode

About IGMP Snooping

IGMP snooping examines IGMP protocol messages to discover which interfaces are connected to hosts or other devices interested in receiving this traffic. Multicast service packets are forwarded only to those hosts listed in the forwarding table. The forwarding table entries are created, maintained, and deleted dynamically based on the host members joining and leaving. IGMP report requests from the ONT are not required to pass the authentication table issued from the OLT, which allows the forwarding table to be updated by directly snooping the IGMP packets. IGMP snooping allows users to watch multicast programs on demand.

About Multicast Group Entry

You can view the multicast group entries learned by the ONT. The HGU type ONT can only be based on global view, and the SFU type ONT is based on port view.

About Multicast Group Learning Limitation

The multicast group learning limitation allows to limit the number of multicast group entries learnt on the ONT. By default, the maximum number of multicast groups learnt on an ONT interface is the maximum number of hardware entries used on an interface. If the number of multicast group entries exceed the configured value, then previous learnt multicast group entries will not be deleted, and new IGMP join messages are dropped. The multicast group limit is configured on the OLT to control the number of multicast group learning on the ONT or ONT port. You must configure the ONT multicast mode before configuring the multicast group limitation.

About Fast Leave

The ONT processes the IGMP leave message in the following ways:

- Normal leave: The local multicast entry is not deleted immediately after the IGMP leave message is received and waits for the multicast query timeout to expire. If an IGMP join message is not received before the multicast query timeout then the local multicast entry is deleted.
- Fast Leave: The local multicast entry is deleted immediately after the IGMP leave message is received and the multicast table resource is freed.

About VLAN tagging on Downlink Multicast Packets

Multicast packets in the downlink path are assigned to a dedicated channel forwarding gemport 4095 on the PON system.

The VLAN tagging on downlink multicast packet feature allows you to configure a VLAN policy on the ONT. Based on the VLAN policy, the ONT performs VLAN tagging on the downlink multicast group packet. The multicast group packet can either be a service packet or a query packet. The packet is then only forwarded to the attached STB device.

The HGU-type ONT is based on the global, and the SFU-type ONT is based on the port.

Configuring VLAN tagging on a downlink multicast packet includes removing a tagging rule, adding a tagging and a translating rule. If VLAN tagging on an uplink multicast packet feature is not configured, then the default flow rule is processed.

How to Configure Multicast in the GPON Network

Configuring IGMP Snooping

To configure IGMP snooping, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**deploy profile line** **Example:** `Device(config)# deploy profile line`	Enters command configuration mode
Step 4	**aim** {*index_num* [**name** *name*] | **name** *name*} **Example:** `Device(deploy-profile-line)# aim 5`	Creates the line profile. • *index_num*: The index of the template. The range is from 0 to M, where M is the maximum number of ONUs supported by the whole machine. • *name*: The name of the template in string. The string length is from 1 to 128.
Step 5	**multicast mode igmp-snooping** [**port** *port_id*] **Example:** `Device(deploy-profile-line)# multicast mode igmp-snooping port 2`	Enables IGMP snooping. *port_id*: The ONT Ethernet port ID. The range is from 1 to 24.

Configuring Multicast Group Learning Limitation

To configure multicast group learning limitation, perform this procedure.

Before you begin

You must configure the ONT multicast mode before configuring this function.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**deploy profile line** **Example:** `Device(config)# deploy profile line`	Enters command configuration mode.

	Command or Action	Purpose
Step 4	**aim** {*index_num* [**name** *name*] | **name** *name*} **Example:** `Device(deploy-profile-line)# aim 5`	Creates the line profile. • *index_num*: The index of the template. The range is from 0 to M, where M is the maximum number of ONUs supported by the whole machine. • *name*: The name of the template in string. The string length is from 1 to 128.
Step 5	[**no**] **multicast group-limit** *num* [**port** {*port_id*}] **Example:** `Device(deploy-profile-line-5)# multicast group-limit 2`	Configures maximum number of multicast groups. • *num*： The maximum multicast group number. The range is from 1 to 128. • *port_id*: The ONT Ethernet port ID. The range is from 1 to 24. Use the **no multicast group-limit** [**port** *port_id*] command to delete this feature.

Configuring Fast Leave

To configure fast leave, perform this procedure.

Before you begin

You must configure the ONT multicast mode before configuring this function.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**deploy profile line** **Example:** `Device(config)# deploy profile line`	Enters command configuration mode.
Step 4	**aim** {*index_num* [**name** *name*] | **name** *name*} **Example:** `Device(deploy-profile-line)# aim 5`	Creates the line profile. • *index_num*: The index of the template. The range is from 0 to M, where M is the maximum number of ONUs supported by the whole machine.

	Command or Action	Purpose
		• *name*: The name of the template in string. The string length is from 1 to 128.
Step 5	[**no**] **multicast fast-leave disable** [**port** *port_id*] **Example:** `Device(deploy-profile-line)# multicast fast-leave disable`	Disables fast leave. *port_id*: The ONT Ethernet port ID. The range is from 1 to 24. Use the **no multicast fast-leave disable** [**port** *port_id*] to enable the fast leave.

Configuring Downlink Multicast Packet Tagging Rule

To configure downlink multicast packet tagging rule, perform this procedure.

Before you begin

You must configure the ONT multicast mode before configuring this function.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**deploy profile line** **Example:** `Device(config)# deploy profile line`	Enters command configuration mode.
Step 4	**aim** {*index_num* [**name** *name*] | **name** *name*} **Example:** `Device(deploy-profile-line)# aim 5`	Creates the line profile. • *index_num*: The index of the template. The range is from 0 to M, where M is the maximum number of ONUs supported by the whole machine. • *name*: The name of the template in string. The string length is from 1 to 128.
Step 5	[**no**] **multicast ds-tag remove** [**port** {*port_id*}] **Example:** `Device(deploy-profile-line-5)# multicast ds-tag remove`	Configures the ONT downlink multicast VLAN tag removing rule. *port_id*: The ONT Ethernet port ID. The range is from 1 to 24.

	Command or Action	Purpose
		Use the **no multicast ds-tag** [**port** *port_id*] to delete the downlink multicast VLAN tag rule.
Step 6	**multicast ds-tag add** *vid* [*priority* | **port** {*port_id*}] **Example:** `Device(deploy-profile-line-5)# multicast ds-tag add 3`	Configures the ONT downlink multicast VLAN tag adding rule. • *vid*: The VLAN ID. The range is from 1 to 4094. • *priority*: The 802.1P priority. The range is from 0 to 7. • *port_id*: The ONT Ethernet port ID. The range is from 1 to 24.
Step 7	**multicast ds-tag translate** *vid* [*priority* | **port** {*port_id*}] **Example:** `Device(deploy-profile-line-5)# multicast ds-tag translate 3`	Configures the ONT uplink multicast VLAN tag translating rule. • *vid*: The VLAN ID. The range is from 1 to 4094. • *priority*: The 802.1P priority. The range is from 0 to 7. • *port_id*: The ONT Ethernet port ID. The range is from 1 to 24.

Monitoring Multicast Entry

The commands in the following table can be used to monitor multicast entry

Table 1: Multicast Entry

Command	Purpose
show ont multicast *ont_id* [**port** *port_id*]	Displays information about multicast learning table on ONT • *port_id*: The ONT Ethernet. The port id is 1 from 24. • *ont_id*： The ONT ID. The slot_num or port_num or ont_id.

Configuration Examples for Multicast in the GPON Network

Example: Configuring IGMP

The following example shows how to configure the SFU multicast working mode to be IGMP snooping. The user's IGMP report can directly trigger establishing multicast forwarding entries through IGMP snooping.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 100
Device(deploy-profile-line-100)# device type c40-100
Device(deploy-profile-line-100)# tcont 1 profile dba 1
Device(deploy-profile-line-100)# gemport 1 tcont 1 vlan-profile 1
Device(deploy-profile-line-100)# mapping 1 vlan 10 gemport 1
Device(deploy-profile-line-1)# multicast mode igmp-snooping port 1
Device(deploy-profile-line-100)# active
Device(deploy-profile-line-100)# end
```

The following example shows how to configure the HGU multicast working mode as IGMP snooping

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 100
Device(deploy-profile-line-100)# device type c30-423
Device(deploy-profile-line-100)# tcont 1 profile dba 1
Device(deploy-profile-line-100)# gemport 1 tcont 1 vlan-profile 1
Device(deploy-profile-line-100)# mapping 1 vlan 10 gemport 1
Device(deploy-profile-line-1)# multicast mode igmp-snooping
Device(deploy-profile-line-100)# active
Device(deploy-profile-line-100)# end
```

The following example shows how to configure the service line profile refer controllable multicast profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 100
Device(deploy-profile-line-100)# device type c40-100
Device(deploy-profile-line-100)# tcont 1 profile dba 1
Device(deploy-profile-line-100)# gemport 1 tcont 1 vlan-profile 1
Device(deploy-profile-line-100)# mapping 1 vlan 10 gemport 1
Saturn(deploy-profile-line-1)# multicast mode olt-control port 1
Device(deploy-profile-line-100)# multicast profile refer 1
Device(deploy-profile-line-100)# active
Device(deploy-profile-line-100)# end
```

The following example shows how to configure the service line profile refer controllable profile.

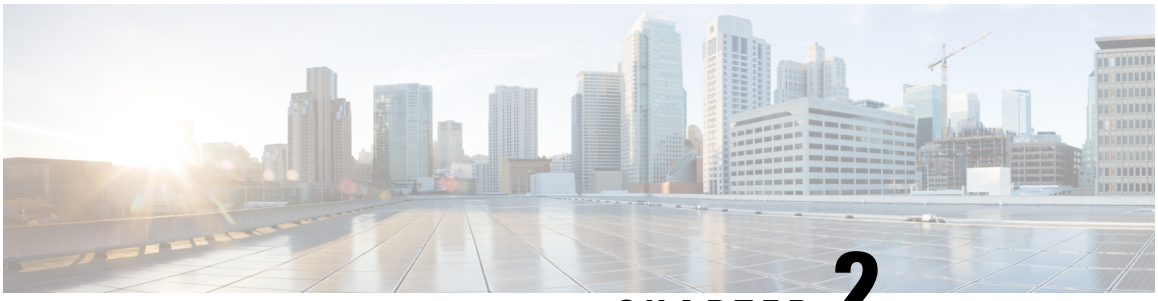
```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 100
Device(deploy-profile-line-100)# device type c30-423
Device(deploy-profile-line-100)# tcont 1 profile dba 1
Device(deploy-profile-line-100)# gemport 1 tcont 1 vlan-profile 1
Device(deploy-profile-line-100)# mapping 1 vlan 10 gemport 1
Device(deploy-profile-line-100)# active
Device(deploy-profile-line-100)# end
#
```

The following example shows how to configure the translate rule of the SFU for upstream multicast packets. IGMP snooping on the OLT learns the multicast group according to the VLAN after the VLAN tag translation.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 100
Device(deploy-profile-line-100)# device type c30-423
Device(deploy-profile-line-100)# tcont 1 profile dba 1
Device(deploy-profile-line-100)# gemport 1 tcont 1 vlan-profile 1
Device(deploy-profile-line-100)# mapping 1 vlan 10 gemport 1
Device(deploy-profile-line-1)# multicast mode igmp-snooping
Device(deploy-profile-line-100)# multicast us-tag translate 10 1
Device(deploy-profile-line-100)# active
Device(deploy-profile-line-100)# end
```

The following example shows how to configure the port of the SFU to untag and forward the downlink multicast packets.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 100
Device(deploy-profile-line-100)# device type c40-100
Device(deploy-profile-line-100)# tcont 1 profile dba 1
Device(deploy-profile-line-100)# gemport 1 tcont 1 vlan-profile 1
Device(deploy-profile-line-100)# mapping 1 vlan 10 gemport 1
Device(deploy-profile-line-1)# multicast mode igmp-snooping port 1
Device(deploy-profile-line-1)# multicast ds-tag remove port 1
Device(deploy-profile-line-100)# active
Device(deploy-profile-line-100)# end
```



CHAPTER 2

Configuring IGMP Snooping

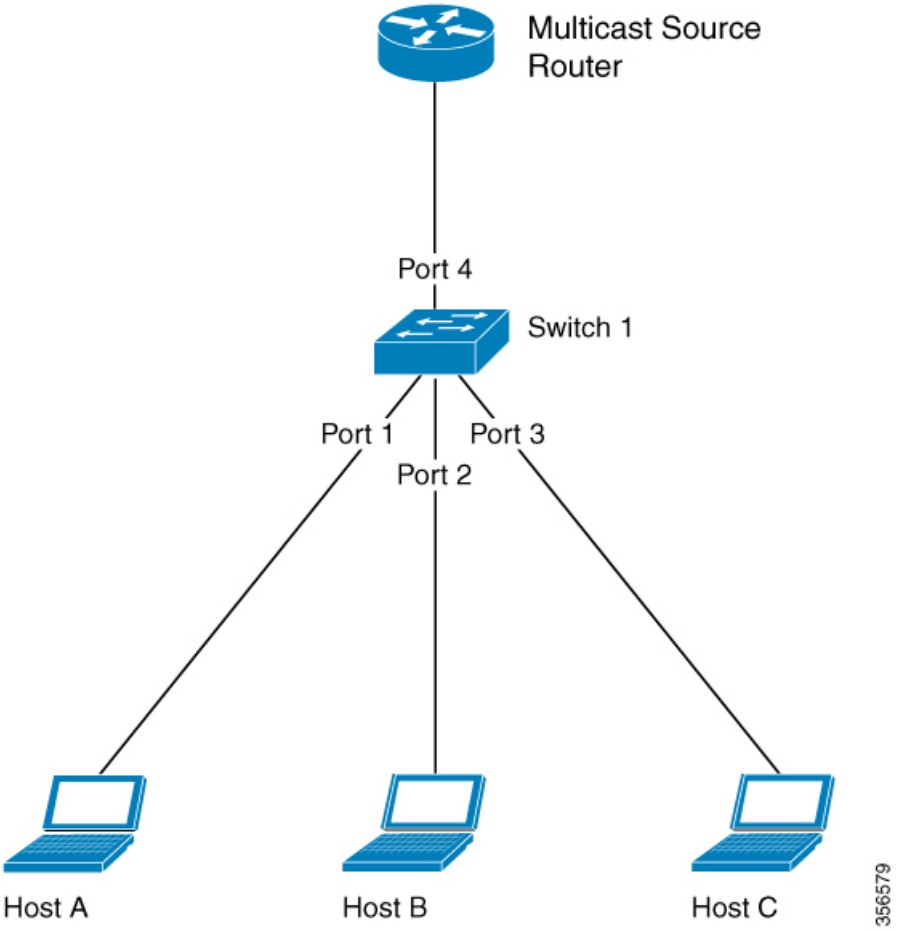
- Information About IGMP Snooping , on page 9
- How to Configure SNMP Snooping, on page 10
- Verifying IGMP Snooping Configuration, on page 21
- Configuration Examples for IGMP Snooping, on page 22

Information About IGMP Snooping

Internet Group Management Protocol (IGMP) is a part of the IP and supports and manages IP multicast between a host and a multicast router. IP multicast allows the transfer of IP data to a host collection formed by a multicast group. The relationships of the multicast group members are dynamic. A host can dynamically add or exit this group to reduce network load to a minimum, and to improve effective data transmission in a network.

IGMP Snooping monitors IGMP packets between a host and routers. It can dynamically create, maintain, and delete a multicast address table. A multicast frame can transfer a packet according to its own multicast address table.

Figure 1: IGMP Snooping Configuration



How to Configure SNMP Snooping

The following topics provide information about the procedures you should perform to configure the IGMP snooping feature.

Enabling IGMP Snooping

To enable IGMP snooping, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**igmp-snooping** **Example:** `Device(config)# igmp-snooping`	Enables IGMP snooping.

Configuring the IGMP Snooping Timer

After receiving an IGMP leave message, IGMP snooping does not delete a port directly from the multicast group. Instead, it waits for a time period before deleting the port from the multicast group. You can configure this time period using the IGMP snooping timer. To configure IGMP snooping timer, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping host-aging-time** *time*
4. **igmp-snooping max-response-time** *time*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**igmp-snooping host-aging-time** *time* **Example:** `Device(config)# igmp-snooping host-aging time 300`	Configures the aging time of dynamic multicast members. By default, the aging time of dynamic multicast member is 300 seconds.
Step 4	**igmp-snooping max-response-time** *time* **Example:**	Configures the maximum response time of IGMP snooping queries. It also configures the maximum waiting time for

	Command or Action	Purpose
	`Device(config)# igmp-snooping max-response-time 10`	deleting group ports after receiving a leave packet. The default setting is 10 seconds.

Configuring Fast Leave

Fast Leave is a feature that allows a port to be removed from a multicast group upon receiving an IGMP Leave message.When you configure Fast Leave, IGMP Snooping removes the port directly from the multicast group upon receiving an IGMP Leave message. Fast Leave helps save bandwidth. To enable Fast Leave, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *port-number*
4. **igmp-snooping fast-leave**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**igmp-snooping fast-leave** **Example:** `Device (config-if)# igmp-snooping fast-leave`	Configures Fast Leave. Note that Fast Leave isn't configured by default. To disable Fast Leave, use the **no igmp-snooping fast-leave** command.

Configuring the Maximum Number of Multicast Groups

To configure the maximum number of multicast groups that an interface or a port can learn, perform this procedure.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface ethernet** *port-number*
4. **igmp-snooping group-limit** *number*
5. **igmp-snooping group-limit action {replace | drop}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**igmp-snooping group-limit** *number* **Example:** `Device(config-if)# igmp-snooping group-limit 20`	Configures the maximum number of multicast groups that the port can learn. IGMP-Snooping group-limit refers to the maximum number of multicast groups which the port can learn. It also refers to the maximum number of multicast groups which the interface can learn. The maximum number for each may be different. To disable the learning of the maximum number of multicast groups, use the **no igmp-snooping group-limit** command.
Step 5	**igmp-snooping group-limit action {replace | drop}** **Example:** `Device(config-if)# igmp-snooping group-limit action replace`	Configures the action that the port performs when it reaches the maximum number of multicast groups it can learn.

What to do next

Note IGMP-Snooping group-limit refers to the maximum number of multicast groups which the port can learn. It also refers to the maximum number of multicast groups which the interface can learn. The maximum number for each may be different.

Configuring the IGMP-Snooping Learning Strategy

You can configure a learning strategy to control the multicast groups that a device learns. If you add a multicast group to the blocked list, the router will not learn the multicast group. If you add a multicast group to the allowed list, the router learns the multicast group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping {permit | deny} {group all | vlan** *vlan-id*}
4. **interface ethernet** *port-number*
5. **igmp-snooping {permit | deny} group-range** *MAC* **multi-count** *multi-count-number***vlan** *vlan-id*
6. **igmp-snooping{permit | deny} {group all | vlan***vlan-list*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**igmp-snooping {permit | deny} {group all | vlan** *vlan-id*} **Example:** `Device(config)# igmp-snooping permit group all`	Configures the default learning rule for multicast groups that are not in the blocked list or the allowed list. By default, the learning rule for all the multicast groups that are not in the blocked list or the allowed list is to learn all the multicast groups.
Step 4	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 5	**igmp-snooping {permit | deny} group-range** *MAC* **multi-count** *multi-count-number***vlan** *vlan-id* **Example:** `Device(config)# igmp-snooping permit group range 01:00:5e:09:08:07 multi-count 12 vlan 1`	Configures the port to learn (or not learn) the range of MAC addresses and VLAN IDs.
Step 6	**igmp-snooping{permit | deny} {group all | vlan***vlan-list*} **Example:** `Device (config)# igmp-snooping permit vlan 1-50`	Configures the port to learn (or not to learn) groups and list of VLAn IDs.

Configuring the IGMP Snooping Querier

You can configure the IGMP snooping querier to enable a Layer 2 switch to send general query packets. The querier sends the packets on the data link layer to establish and maintain multicast forwarding entries. You can also configure the IGMP snooping querier to send VLANs, source addresses, maximum response times, and query cycles for general queries. To configure the IGMP snooping querier, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping querier**
4. **igmp-snooping querier version** *version-id*
5. **igmp-snooping querier-vlan** *vlan-list*
6. **igmp-snooping query-interval** *interval*
7. **igmp-snooping query-max-respond** *time*
8. **igmp-snooping general-query source-ip** *ip-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**igmp-snooping querier** **Example:** `Device(config)# igmp-snooping querier`	Enables the IGMP snooping querier. Disable the IGMP snooping querier by using the **no igmp-snooping querier** command.
Step 4	**igmp-snooping querier version** *version-id* **Example:** `Device(config)# igmp-snooping querier version 2`	Configures the version of the querier. The default version is version 2.
Step 5	**igmp-snooping querier-vlan** *vlan-list* **Example:** `Device(config)# igmp-snooping querier-vlan 1-50`	Configures VLANs for general query packets. Disable the VLAN configurations for the general query packets by using the **no igmp-snooping querier-vlan** command.
Step 6	**igmp-snooping query-interval** *interval* **Example:** `Device(config)# igmp-snooping query-interval 500`	Configures the interval, in seconds, for sending the general query packets. The range is 1 to 30000 seconds. Disable the interval for sending general query packets by using the **no igmp-snooping query-interval** command.

	Command or Action	Purpose
Step 7	**igmp-snooping query-max-respond** *time* **Example:** `Device(config)# igmp-snooping query-max-respond 10`	Configures the maximum response time, in seconds, for the general query packets. The range is 1to 25 seconds. Disable the maximum response time configuration for general query packets by using the **no igmp-snooping query-max-respond** command.
Step 8	**igmp-snooping general-query source-ip** *ip-address* **Example:** `Device(config)# igmp-snooping general-query source-ip 192.0.2.255`	Configures the source IP address for sending general query packets. Disable the source IP address for sending general query packets by using the **no igmp-snooping general-query source-ip** command.

Configuring the Route Port

The route port is automatically added to the dynamic multicast group learned by IGMP snooping. The route port is able to forward multicast traffic packets. When the device receives a membership report from a host, the device forwards the report to the route port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping route-port forward**
4. **igmp-snooping router-port-age {on | off | age-time}**
5. **igmp-snooping route-port vlan** *vlan-id* **interface{all | channel-group** *channel-group-id* **| ethernet** *interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**igmp-snooping route-port forward** **Example:** `Device(config)# igmp-snooping route-port forward`	Configures the hybrid route function. Disable the hybrid route function by using the **no igmp-snooping route-port forward** command.
Step 4	**igmp-snooping router-port-age {on	off	age-time}** **Example:**	Configures the aging time, in seconds, for the dynamic route port. The aging time is set to 300 seconds by default.

	Command or Action	Purpose
	`Device(config)# igmp-snooping router-port-age on`	Disable the aging time of the dynamic route port by using the **no igmp-snooping router-port-age** command.
Step 5	**igmp-snooping route-port vlan** *vlan-id* **interface**{**all** | **channel-group** *channel-group-id* | **ethernet** *interface-number* **Example:** `Device(config)# igmp-snooping route-port vlan 50 interface all`	Configures a static route port. Disable the static route port using the **no igmp-snooping route-port** command.

Configuring a Multicast VLAN for Internet Group Management Protocol Packets

After you enable the multicast VLAN function on a port, the device modifies the VLAN of the Internet Group Management Protocol (IGMP) packets to a multicast VLAN. This is regardless of the VLAN to which the received IGMP packets belong. To configure a multicast VLAN for IGMP packets, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *port-number*
4. **igmp-snooping multicast vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**igmp-snooping multicast vlan** *vlan-id* **Example:** `Device(config-if)# igmp-snooping multicast vlan 50`	Configures the multicast VLAN for the port. Disable the multicast VLAN for the port by using the **no igmp-snooping multicast vlan** command.

Configuring a Port to Record the Host MAC Address

To enable the recording of the MAC address of the source of an IGMP report packet, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *port-number*
4. **igmp-snooping record-host**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**igmp-snooping record-host** **Example:** `Device(config)# igmp-snooping record-host`	Configures the port to record the host MAC address. Disable the recording of the host MAC address using the **no igmp-snooping record-host** command.

Configuring the Suppression of a Multicast Report

When you enable IGMP snooping suppression of multicast reports, the following changes take place:

- Each multicast group sends only one multicast report to the mroute port. When the first report is received, the source MAC address is replaced with the MAC address from the device. The report is forwarded to the mroute port. This report is not forwarded to the client. If another multicast report is received from the same group later, only the local member or timer information is updated. The report is not forwarded to the mroute port.
- After receiving a general query, the device encapsulates all the packets in the report packet and forwards it to the mroute port. The mroute port then forwards the query to all the clients. When receiving a specific query, the device encapsulates the specified group into a report packet and sends it to the mroute port. The mroute port then forwards the query to the specified client. If the device has not learnt the specified group, it discards the query.
- After receiving a leave report, the member that sent the leave report is deleted. If there are other members in the multicast group a report is not sent to the mroute port. If the member sending the leave report is

the last member to leave the multicast group, the source MAC address is replaced with the device MAC address and the report is forwarded to the mroute port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping report-suppresion**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**igmp-snooping report-suppresion** **Example:** `Device(config)# igmp-snooping report-suppression`	Configures the suppression of multicast reports. Disable the suppression of multicast reports by using the **no igmp-snooping report-suppression** command.

Configuring the Dropping of Query and Report Packets

By default, ports receive all IGMP packets. To configure a port to drop query or report packets, perform this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *port-number*
4. **igmp-snooping drop {query | report}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**igmp-snooping drop {query | report}** **Example:** `Device(conif-if)# igmp-snooping drop query`	Configures the port to drop IGMP query or report packets. Enable the port to start receiving IGMP query or report packets by using the **no igmp-snooping drop query** command.

Configuring the IGMP Snooping Blocked List and Allowed List Profiles

IGMP snooping provides blocked list and allowed list profiles. You can create several profiles in global configuration mode, and then configure the profile list referenced by the corresponding port under interface configuration mode. You can configure the type and range of the IGMP snooping profile. An IGMP snooping profile takes effect only when it is referenced by a port. To configure a port to reference a profile, specify the same profile for multiple ports. A port can reference only one type of profile, for example, permit or deny.

- When a port references the permit profile, it can learn only the multicast groups defined by the permit profile.
- When a port references a deny profile, it can learn all the multicast groups, except the ones defined in the deny profile.
- If the port does not reference any profile, it learns all the multicast groups as usual.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **igmp-snooping profile** *profile-id*
4. **profile limit {permit | deny}**
5. **ip range** *start-ip-address end-ip-address* **vlan** *vlan-id*
6. **mac range** *start-mac-address end-mac-address* **vlan** *vlan-id*
7. **interface ethernet** *port-number*
8. **igmp-snooping profile refer** *profile-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**igmp-snooping profile** *profile-id* **Example:** `Device(config)# igmp-snooping profile 1`	Creates an IGMP snooping profile. Enters profile configuration mode. Disable profile configuration using **no igmp-snooping profile** command.
Step 4	**profile limit** {**permit** | **deny**} **Example:** `Device(config-igmp-profile)# profile limit permit`	Configures the profile type.
Step 5	**ip range** *start-ip-address end-ip-address* **vlan** *vlan-id* **Example:** `Device(config-igmp-profile)# ip range 224.0.0.1 239.255.255.254 vlan 10`	Configures the range of IP addresses and VLAN IDs for the profile. The IP address range is from 224.0.0.1 to 239.255.255.254. The VLAN ID range is from 1 to 4094.
Step 6	**mac range** *start-mac-address end-mac-address* **vlan** *vlan-id* **Example:** `Device(config-igmp-profile)# mac range 01:00:5e:09:08:07 01:00:5e:09:09:08 vlan 10`	Configures the range of MAC addresses and VLAN IDs for the profile. The VLAN ID range is from 1 to 4094.
Step 7	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 8	**igmp-snooping profile refer** *profile-list* **Example:** `Device(config-if)# igmp-snooping profile refer 1-5`	Configures the profile reference of the port. Disable the profile reference of a port using the **no igmp-snooping profile refer** command.

Verifying IGMP Snooping Configuration

To verify the IGMP snooping configuration, run these commands, as required.

Command	Description
show igmp-snooping	Displays IGMP snooping configurations.
show igmp-snooping router-dynamic	Displays a dynamic route port
show igmp-snooping router-static	Displays a static route port
igmp-snooping statistics {**interface** [**all** | **ethernet** *ethernet-port-id* | **GPON** *GPON-port-id*] **vlan**}	Displays the statistics of igmp-snooping packets.
show igmp-snooping record-host [*interface*]	Displays the MAC address of a record host.
show igmp-snooping profile	Displays the configurations of a profile.
show multicast	Displays a multicast table.

Command	Description
show multicast igmp-snooping interface	Displays detailed information about a multicast table.

Configuration Examples for IGMP Snooping

The following sections provide examples of IGMP snooping configurations.

Example: Enabling IGMP Snooping

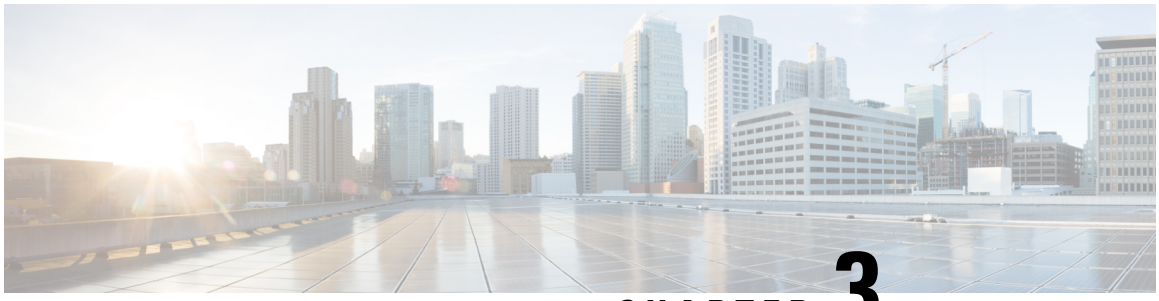
The following example shows how to enable IGMP snooping on a device. The example also shows how to add Ethernet 0 / 1, Ethernet 0 / 2, and Ethernet 0 / 3 to VLAN 2, VLAN 3, and VLAN 4 respectively.

```
Device(config)# igmp-snooping
Device(config)# vlan 2
Device(config-if-vlan)# switchport ethernet 1/1
Device(config-if-vlan)# exit
Device(config)# vlan 3
Device(config-if-vlan)# switchport ethernet 1/2
Device(config-if-vlan)# exit
Device(config)# vlan 4
Device(config-if-vlan)# switchport ethernet 1/3
Device(config-if-vlan)# exit
```

Example: Displaying the Multicast Group Learnt by a Device

The following example shows how to display the multicast groups learnt by a device:

```
Device(config)# show multicast
show multicast table information
MAC Address       : 01:00:5e:00:01:01
VLAN ID           : 2
Static port list        :.
IGMP port list       : e1/1
Dynamic port list     :

MAC Address       : 01:00:5e:00:01:02
VLAN ID           : 3
Static port list        :.
IGMP port list       : e1/2
Dynamic port list     :

MAC Address       : 01:00:5e:00:01:03
VLAN ID           : 4
Static port list        :
IGMP port list       : e1/3.
Dynamic port list     :

Total entries: 3 .
Switch (config)#show igmp-snooping router-dynamic
  Port        VID     Age       Type
  e1/4       2       284      { STATIC }
  e1/4       3       284      { STATIC }s
  e1/4       4       284      { STATIC }

Total Record: 3
```



CHAPTER 3

Configuring MLD Snooping

- Information About MLD Snooping, on page 23
- How to Configure MLD Snooping, on page 23
- Verifying MLD Snooping Configuration, on page 29
- Configuration Example for MLD Snooping, on page 30

Information About MLD Snooping

Multicast Listener Discovery (MLD) is part of the IPv6 protocol to support and manage IPv6 multicast between a host and the multicast router. IP multicast allows IP datagrams to be transmitted to a set of hosts that make up a multicast group. Hosts can dynamically join or leave multicast groups to minimize network load and to achieve effective data transmission.

MLD snooping monitors the MLD packets between a host and the router. MLD snooping dynamically creates, maintains, and deletes the multicast address table based on the joining and leaving of the multicast group members. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets and maintained in a multicast address table.

How to Configure MLD Snooping

The following sections provide configuration information about MLD snooping.

Enabling MLD Snooping

To enable MLD Snooping on the device, perform the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**mld-snooping** **Example:** `Device(config)# mld-snooping`	Enables MLD snooping on the device.

Configuring MLD Snooping Timer

To configure MLD Snooping timer, perform the following procedure:

SUMMARY STEPS

1. **configure terminal**
2. **mld-snooping host-aging-time** *time*
3. **mld-snooping max-response-time** *time*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**mld-snooping host-aging-time** *time* **Example:** `Device(config)# mld-snooping host-aging-time 1000`	Configures the aging time of dynamic multicast ports. By default, the aging time of a dynamic multicast port is 300 seconds.
Step 3	**mld-snooping max-response-time** *time* **Example:** `Device(config)# mld-snooping max-response-time 7`	Configures the maximum response time of the leave packets. By default, the maximum response time of leave packets is 10 seconds.

Configuring Fast-Leave

Fast Leave feature allows a port to be immediately removed from a multicast group upon receiving a leave packet on that port. If the Fast Leave feature is not enabled, MLD Snooping waits for a period of time before removing the port from the multicast group. Enabling the Fast Leave feature when there is only one user on the port provides for effective bandwidth utilization.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *interface-num*
3. **mld-snooping fast-leave**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface ethernet** *interface-num* **Example:** `Device(config)# interface ethernet 1/1`	Enters the interface configuration mode.
Step 3	**mld-snooping fast-leave** **Example:** `Device(config-if-ethernet-1/1)# mld-snooping fast-leave`	Enables the Fast Leave feature on the port. To disable Fast Leave, use the **no mld-snooping fast-leave** command. By default, Fast Leave is disabled on the device.

Configuring Maximum Multicast Groups on a Port

To set the maximum number of multicast groups that a port can join, perform the following procedure.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *interface-num*
3. **mld-snooping group-limit** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**interface ethernet** *interface-num* **Example:** `Device(config)#interface ethernet 1/1`	Enters the interface configuration mode.
Step 3	**mld-snooping group-limit** *number* **Example:** `Device(config-if)#mld-snooping group-limit 100`	Specifies the maximum number of multicast groups that the interface can join. By default, the maximum number of multicast groups on an interface is the largest number of multicast packets that a device can learn.

Configuring Multicast Learning Strategy of MLD Snooping

You can configure a multicast learning strategy to allow the device to discover only specific multicast groups. The device can discover only those multicast groups that are a part of allowed list. Multicast groups that are a part of blocked list are not discovered by the device.

SUMMARY STEPS

1. **configure terminal**
2. **mld-snooping** { **permit** | **deny**} {**group all** | **vlan** *vlanid*}
3. **interface ethernet** *interface-num*
4. **mld-snooping** { **permit** | **deny**}**group-range** *MAC* **multi-count** *num* **vlan** *vlanid*
5. **mld-snooping** { **permit** | **deny**}**group** *MAC* **vlan** *vlanid*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**mld-snooping** { **permit**	**deny**} {**group all**	**vlan** *vlanid*} **Example:** `Device(config)#mld-snooping permit vlan 2`	Specifies a learning rule on the device for the multicast groups that are not a part of blocked list or the allowed list. By default, the device discovers all those multicast groups that are not part of the blocked list or the allowed list.
Step 3	**interface ethernet** *interface-num* **Example:** `Device(config)#interface ethernet 1/1`	Enters the interface configuration mode.
Step 4	**mld-snooping** { **permit**	**deny**}**group-range** *MAC* **multi-count** *num* **vlan** *vlanid* **Example:** `Device(config-if-ethernet-1/1)# mld-snooping permit group-range 33:33:5e:09:08:07 multi-count 5 vlan 4`	Specifies the list of multicast groups that are permitted or denied by MLD snooping in the particular VLAN for the given range of MAC addresses.
Step 5	**mld-snooping** { **permit**	**deny**}**group** *MAC* **vlan** *vlanid* **Example:** `Device(config-if-ethernet-1/1)# mld-snooping permit group 33:33:5e:09:08:07 vlan 5`	Specifies the list of multicast groups that are permitted or denied by MLD snooping in the particular VLAN.

Configuring MLD Snooping Querier

In a network where IP multicast routing is configured, the IP multicast router acts as the MLD querier. If the IP multicast traffic in a VLAN only needs to be Layer 2 switched, an IP multicast router is not required, but

without an IP multicast router on the VLAN, you must configure another switch as the MLD querier so that it can send queries.

When enabled, the MLD snooping querier sends out periodic MLD queries that trigger MLD report messages from the device that wants to receive IP multicast traffic. MLD snooping listens to these MLD reports to establish appropriate forwarding.

You can enable the MLD snooping querier on all the devices in the VLAN, but for each VLAN that is connected to devices that use MLD to report interest in IP multicast traffic, you must configure at least one device as the MLD snooping querier.

You can configure the MLD snooping querier to forward the source address, maximum response time, and query interval for sending general query messages.

SUMMARY STEPS

1. **configure terminal**
2. **mld-snooping querier**
3. **mld-snooping query-interval** *interval*
4. **mld-snooping query-max-respond** *time*
5. **mld-snooping querier-vlan** *vlanid*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**mld-snooping querier** **Example:** `Device(config)#mld-snooping querier`	Enables the MLD snooping querier.
Step 3	**mld-snooping query-interval** *interval* **Example:** `Device(config)#mld-snooping query-interval 1000`	Specifies the time period that the device waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. Valid query interval is 1 to 30000 seconds.
Step 4	**mld-snooping query-max-respond** *time* **Example:** `Device(config)#mld-snooping query-max-respond 10`	Specifies the maximum response time for the general query packets. Valid values are 1 to 25 seconds.
Step 5	**mld-snooping querier-vlan** *vlanid* **Example:** `Device(config)#mld-snooping querier-vlan 3`	Specifies the VLAN that carries the general query packets.

Configuring a Routing Port

You can add a router port to the dynamic multicast so that the routing port also forwards the multicast traffic packets. To configure a multicast routing port, perform the following procedure.

SUMMARY STEPS

1. **configure terminal**
2. **mld-snooping route-port forward**
3. **mld-snooping router-port-age** {**on** | **off** | *age-time*}
4. **mld-snooping route-port vlan** *vlanid* **interface** {**all** | **ethernet** *interface-num* }

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**mld-snooping route-port forward** **Example:** `Device(config)#mld-snooping route-port forward`	Configures the routing port to forward mutlicast traffic.
Step 3	**mld-snooping router-port-age** {**on** | **off** | *age-time*} **Example:** `Device(config)# mld-snooping router-port-age on`	Configures the aging time of the dynamic routing port, in seconds.
Step 4	**mld-snooping route-port vlan** *vlanid* **interface** {**all** | **ethernet** *interface-num* } **Example:** `Device(config)#mld-snooping route-port vlan 5 interface all`	Configures the mutlicast router VLAN ID and specifies the interface to the multicast router.

Configuring a Multicast VLAN

You can configure multicast VLAN on a port, which ensures a more efficient distribution of multicast packets across the network. After the multicast VLAN feature is enabled on a port, the device forwards the MLD packets to the multicast VLAN regardless of the VLAN to which the MLD packets belong.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *interface-num*
3. **mld-snooping multicast vlan** *vlanid*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**interface ethernet** *interface-num* **Example:** `Device(config)#interface ethernet 1/1`	Enters the interface configuration mode.
Step 3	**mld-snooping multicast vlan** *vlanid* **Example:** `Device(config-if)# mld-snooping multicast vlan 9`	Configures a multicast VLAN on the interface. You can disable the mutlicast VLAN for a port using the **no** form the command.

Configuring a Port to Record Host MAC Address

To enable the recording of MAC address of the source of an MLD report packet, perform the following procedure.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *interface-num*
3. **mld-snooping record-host**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface ethernet** *interface-num* **Example:** `Device(config)# interface ethernet 1/1`	Enters the interface configuration mode.
Step 3	**mld-snooping record-host** **Example:** `Device(config-if)# mld-snooping record-host`	Configures the port to record the host MAC address.

Verifying MLD Snooping Configuration

To verify the MLD snooping configuration, run these commands, as required.

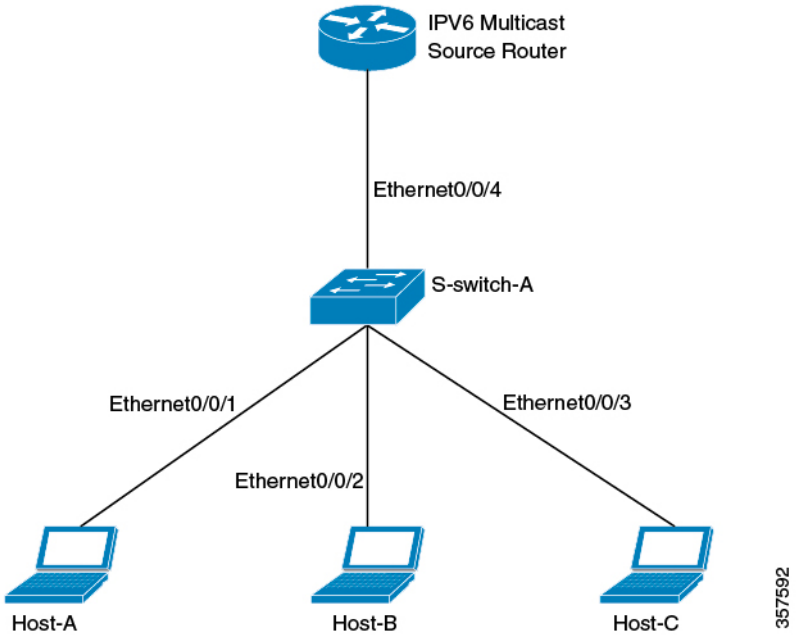
Command	Description
show mld-snooping	Displays MLD snooping configurations.
show mld-snooping router-dynamic	Displays dynamic router ports.
show mld-snooping router-static	Displays static route ports.
show multicast mld-snooping interface { **ethernet** *interface-num* | **gpon** *interface-num* }	Displays information about the multicast group.

Configuration Example for MLD Snooping

Network Requirements

Consider a network topology wherein hosts Host-A, Host-B, and Host-C belong to VLAN 2, VLAN 3, and VLAN 4 respectively. The hosts are configured to receive the data of the multicast group with the address FF02::01::0101, FF02::01::0102 and FF02::01::0103 respectively.

Figure 2: MLD Snooping Configuration



Configuration Steps

1. Configure S-switch-A

   Configure VLAN 2, VLAN 3 and VLAN 4, and then add Ethernet 0/0/1, Ethernet 0/0/2 and Ethernet 0/0/3 to VLAN 2, VLAN 3, and VLAN 4 respectively.

```
S-switch-A(config)# vlan 2
S-switch-A(config-if-vlan)# switchport ethernet 0/0/1
S-switch-A(config-if-vlan)# exit
```

```
S-switch-A(config)# vlan 3
S-switch-A(config-if-vlan)# switchport ethernet 0/0/2
S-switch-A(config-if-vlan)# exit
S-switch-A(config)# vlan 4
S-switch-A(config-if-vlan)# switchport ethernet 0/0/3
S-switch-A(config-if-vlan)# exit
```

2. Enable MLD Snooping

```
S-switch-A(config)# mld-snooping
```

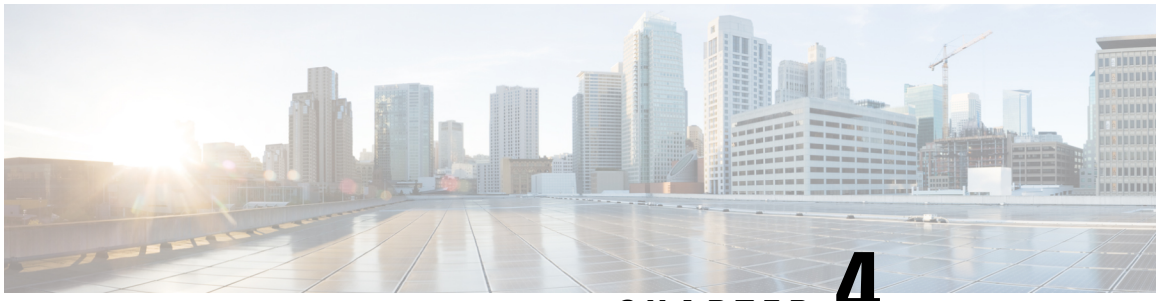
When Host-A, Host-B, and Host-C send MLD report packets to S-switch-A, S-switch-A learns the corresponding multicast group entries. When the IPv6 Multicast Source Router sends MLD query packets to S-switch-A, S-switch-A learns the corresponding routing port entries.

3. Display and verify the multicast groups learned by S-switch-A

```
S-switch-A(config)# show multicast mld-snooping interface
show mld-snooping multicast table information
MAC Address : 33:33:00:01:00:01
IP Address   :  FF02::01::0101
VLAN ID     : 2
Aging time: 297
MLD Port   : e1/1
MLD Version: V1, V2

MAC Address : 33:33:00:01:00:02
IP Address   :  FF02::01::0102
VLAN ID     : 3
Aging time: 290
MLD Port   : e1/1
MLD Version: V1, V2
.

MAC Address : 33:33:00:01:00:03
IP Address   :  FF02::01::0103
VLAN ID     : 4
Aging time: 281
MLD Port   : e1/1
MLD Version: V1, V2

Total entries: 3 .
```

```
S-switch-A(config)# show mld-snooping router-dynamic
  Port        VID     Age       Type
  e0/0/4       2       284      { QUERY }
  e0/0/4       3       284      { QUERY }
  e0/0/4       4       284      { QUERY }
Total Record: 3
```

When a Multicast Source Router sends the multicast data stream FF02::01::0101, FF02::01::0102 and FF02::01::0103, S-switch-A distributes the corresponding data stream to Host-A, Host-B and Host-C.



CHAPTER 4

Configuring Static Multicast Tables

- Information About Static Multicast Tables, on page 33
- How to Configure Static Multicast Tables, on page 33
- Configuration Examples for Static Multicast Tables, on page 35

Information About Static Multicast Tables

You can manually configure the addresses in a multicast table. Such a table is a static multicast table. A static multicast MAC table won't age and it won't be lost after it's saved. At present, you can configure only IPv4 multicast entries in a static multicast table.

How to Configure Static Multicast Tables

The following topics provide information about the procedures that you can perform to configure static multicast tables.

Configuring a Static Multicast Group

To create a static multicast group, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **multicast** {**mac-address** *mac-address* | **ip-address** *ip-address*}**vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**multicast** {**mac-address** *mac-address* | **ip-address** *ip-address*}**vlan** *vlan-id* **Example:** `Device(config)# multicast ip-address 224.1.1.100 vlan 10`	Creates a static multicast group.

Adding a Port to a Static Multicast Group

To add a port to a static multicast group, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **multicast** {**mac-address** *mac-address* | **ip-address** *ip-address*}**vlan** *vlan-id* **interface** {**all** | *interface-list*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**multicast** {**mac-address** *mac-address* | **ip-address** *ip-address*}**vlan** *vlan-id* **interface** {**all** | *interface-list*} **Example:** `Device(config)# multicast ip-address 224.1.1.100 vlan 10 interface all`	Adds a port to a static multicast group.

Configuring a Proxy Port

When a device is configured with a static multicast table, you can configure a proxy port on the device. The proxy port will send the multicast report to the multicast source.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **multicast** {**mac-address** *mac-address* | **ip-address** *ip-address*} **vlan** *vlan-id* **proxy-port ethernet** *interface-list*
4. **multicast proxy-interval** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**multicast** {**mac-address** *mac-address*	**ip-address** *ip-address*} **vlan** *vlan-id* **proxy-port ethernet** *interface-list* **Example:** `Device(config)# multicast ip-address 224.1.1.111 vlan 100 proxy-port ethernet 1/3 to ethernet 1/4`	Creates a proxy port for a static multicast group.
Step 4	**multicast proxy-interval** *seconds* **Example:** `Device(config)# multicast proxy-interval 100`	Configures the interval at which the device sends report packets to the multicast source through the proxy port. The range is 1 to 300 seconds. The default value is 10 seconds.

Configuration Examples for Static Multicast Tables

The following topics provide examples of static multicast table configurations.

Example: Creating a Static Multicast Group

The following example shows how to create a static multicast group for a MAC address. The MAC address is 01: 00: 5e: 01: 02: 03 and the VLAN ID is 1:

```
Device(config)# multicast mac-address 01:00:5e:01:02:03 vlan 1
```

The following example shows how to create a static multicast group for an IP address. The IP address is 224.0.1.1 and VLAN ID is 1:

```
Device(config)# multicast ip-address 224.0.1.1 vlan 1
```

Example: Adding a Port to a Static Multicast Group

The following example shows how to add the Ethernet ports 2, 3, and 4 to a static multicast group.

```
Device(config)# multicast mac-address 01:00:5e:01:02:03 vlan 1 interface ethernet 1/2 to ethernet 1/4
```