CHAPTER 34

Configuring IPv6 MLD Snooping

Note To use IPv6 MLD Snooping, the switch must be running the LAN Base image.

You can use Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP version 6 (IPv6) multicast data to clients and routers in a switched network on the Catalyst 2960 switch.

To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the **sdm prefer dual-ipv4-and-ipv6 default**

For related information, see these chapters:

- Chapter 7, "Configuring SDM Templates."

  For information about IPv6 on the switch, see Chapter 33, "Configuring IPv6 Host Functions."

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

This chapter includes these sections:

Understanding MLD Snooping

In IP version 4 (IPv4), Layer 2 switches can use Internet Group Management Protocol (IGMP) snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. In IPv6, MLD snooping performs a similar function. 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.

packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2 and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch supports two versions of MLD snooping:

MLDv1 snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination multicast addresses.

MLDv2 basic snooping (MBSS) uses MLDv2 control packets to set up traffic forwarding based on IPv6 destination multicast addresses.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast addresses.

The switch does not support MLDv2 enhanced snooping (MESS), which sets up IPv6 source and destination multicast address-based forwarding.

MLD snooping can be enabled or disabled globally or per VLAN. When MLD snooping is enabled, a per-VLAN IPv6 multicast MAC address table is constructed in software and a per-VLAN IPv6 multicast address table is constructed in software and hardware. The switch then performs IPv6 multicast-address based bridging in hardware.

These sections describe some parameters of IPv6 MLD snooping:

MLD Messages

-
-
-

MLD Queries

Note

Multicast Client Aging Robustness

Multicast Router Discovery

-
-
-
-
-

-
-

MLD Reports

The processing of MLDv1 join messages is essentially the same as with IGMPv2. When no IPv6 multicast routers are detected in a VLAN, reports are not processed or forwarded from the switch. When IPv6 multicast routers are detected and an MLDv1 report is received, an IPv6 multicast group address and an IPv6 multicast MAC address are entered in the VLAN MLD database. Then all IPv6 multicast traffic to the group within the VLAN is forwarded using this address. When MLD snooping is disabled, reports are flooded in the ingress VLAN.

When MLD snooping is enabled, MLD report suppression, called listener message suppression, is automatically enabled. With report suppression, the switch forwards the first MLDv1 report received by a group to IPv6 multicast routers; subsequent reports for the group are not sent to the routers. When MLD snooping is disabled, report suppression is disabled, and all MLDv1 reports are flooded to the ingress VLAN.

The switch also supports MLDv1 proxy reporting. When an MLDv1 MASQ is received, the switch responds with MLDv1 reports for the address on which the query arrived if the group exists in the switch on another port and if the port on which the query arrived is not the last member port for the address.

MLD Done Messages and Immediate-Leave

ipv6 mld snooping last-listener-query count

ipv6 mld snooping last-listener-query-interval

Topology Change Notification Processing

Configuring IPv6 MLD Snooping

-
-
-
-
-
-
-
-

Default MLD Snooping Configuration

Table 34-1 Default MLD Snooping Configuration

Feature	Default Setting
	Note
	Note

Default MLD Snooping Configuration (continued)

Last listener query interval	Global: 1000 (1 second); VLAN: 0. **Note** The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global interval.
TCN query solicit	Disabled.
TCN query count	2.
MLD listener suppression	Enabled.

MLD Snooping Configuration Guidelines

-
-
-
-

Enabling or Disabling MLD Snooping

Beginning in privileged EXEC mode, follow these steps to globally enable MLD snooping on the switch:

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Note

configure terminal	
ipv6 mld snooping	
ipv6 mld snooping vlan *vlan-id*	
end	
copy running-config startup-config	

vlan-id

.

configure terminal	
ipv6 mld snooping vlan *vlan-id* **static** *ipv6_multicast_address* *interface-id*	*vlan-id* *ipv6_multicast_address* *interface-id*

show ipv6 mld snooping multicast-address user **show ipv6 mld snooping multicast-address vlan user**	
copy running-config startup-config	

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet0/1
                end
```

configure terminal	
ipv6 mld snooping vlan mrouter interface	
end	
show ipv6 mld snooping mrouter [ ]	Verify that IPv6 MLD snooping is enabled on the VLAN interface.
	(Optional) Save your entries in the configuration file.

```
configure terminal
        ipv6 mld snooping vlan 200 mrouter interface gigabitethernet0/2
        exit
```

When you enable MLDv1 Immediate Leave, the switch immediately removes a port from a multicast group when it detects an MLD Done message on that port. You should only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN. When there are multiple clients for a multicast group on the same port, you should not enable Immediate-Leave in a VLAN.

Beginning in privileged EXEC mode, follow these steps to enable MLDv1 Immediate Leave:

To disable MLD Immediate Leave on a VLAN, use the
global configuration command.

This example shows how to enable MLD Immediate Leave on VLAN 130:

```
ipv6 mld snooping vlan 130 immediate-leave
exit
```

ipv6 mld snooping robustness-variable	
ipv6 mld snooping vlan robustness-variable	
ipv6 mld snooping last-listener-query-count *count*	

	Command	Purpose
Step 6		
Step 7		
Step 8		
Step 9		
Step 10		
Step 11		
Step 12		

```
        ipv6 mld snooping vlan 200 last-listener-query-count 3
        exit


configure terminal
        ipv6 mld snooping last-listener-query-interval 2000
        exit
```

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Displaying MLD Snooping Information

Table 34-2 Commands for Displaying MLD Snooping Information

Table 34-2 Commands for Displaying MLD Snooping Information (continued)

| |	
vlan-id ipv6-multicast-address	