



Configuring MLD Snooping for IPv6 Multicast Traffic

This chapter describes how to configure Multicast Listener Discovery (MLD) snooping for IPv6 multicast traffic in Cisco IOS Release 12.2SX.



Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:
http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
- To constrain IPv4 multicast traffic, see [Chapter 38, “Configuring IGMP Snooping for IPv4 Multicast Traffic.”](#)
- PFC3C and PFC3CXL modes support MLD version 1 (MLDv1) and MLD version 2 (MLDv2).
- These modes support only MLD version 2 (MLDv2):
 - PFC3A
 - PFC3B
 - PFC3BXL



Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
[Participate in the Technical Documentation Ideas forum](#)

This chapter consists of these sections:

- [Understanding MLD Snooping, page 36-2](#)
- [Default MLD Snooping Configuration, page 36-8](#)
- [MLD Snooping Configuration Guidelines and Restrictions, page 36-8](#)
- [MLD Snooping Querier Configuration Guidelines and Restrictions, page 36-9](#)
- [Enabling the MLD Snooping Querier, page 36-9](#)
- [Configuring MLD Snooping, page 36-10](#)

Understanding MLD Snooping

These sections describe MLD snooping:

- [MLD Snooping Overview, page 36-2](#)
- [MLD Messages, page 36-3](#)
- [Source-Based Filtering, page 36-3](#)
- [Explicit Host Tracking, page 36-3](#)
- [MLD Snooping Proxy Reporting, page 36-4](#)
- [Joining an IPv6 Multicast Group, page 36-4](#)
- [Leaving a Multicast Group, page 36-6](#)
- [Understanding the MLD Snooping Querier, page 36-7](#)

MLD Snooping Overview

MLD snooping allows the switch to examine MLD packets and make forwarding decisions based on their content.

You can configure the switch to use MLD snooping in subnets that receive MLD queries from either MLD or the MLD snooping querier. MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

MLD, which runs at Layer 3 on a multicast router, generates Layer 3 MLD queries in subnets where the multicast traffic needs to be routed. For information about MLD, see this publication:

<http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ipv6-12-2sx-book.html>

You can configure the MLD snooping querier on the switch to support MLD snooping in subnets that do not have any multicast router interfaces. For more information about the MLD snooping querier, see the “[Enabling the MLD Snooping Querier](#)” section on page 36-9.

MLD (on a multicast router) or, locally, the MLD snooping querier, sends out periodic general MLD queries that the switch forwards through all ports in the VLAN, and to which hosts respond. MLD snooping monitors the Layer 3 MLD traffic.



Note

PFC/DFC 3C/3CXL supports source-only Layer 2 entries, but PFC/DFC 3B/3BXL does not support source-only Layer 2 entries and therefore IPv6 multicast flooding cannot be prevented in a source-only network.



Note

If a multicast group has only sources and no receivers in a VLAN, MLD snooping constrains the multicast traffic to only the multicast router ports.

MLD Messages

These are the MLD messages:

- Multicast listener queries
 - General query—Sent by a multicast router to learn which multicast addresses have listeners.
 - Multicast address specific query—Sent by a multicast router to learn if a particular multicast address has any listeners.
 - Multicast address and source specific query—Sent by a multicast router to learn if any of the sources from the specified list for the particular multicast address has any listeners.
- Multicast listener reports
 - Current state record (solicited)—Sent by a host in response to a query to specify the INCLUDE or EXCLUDE mode for every multicast group in which the host is interested.
 - Filter mode change record (unsolicited)—Sent by a host to change the INCLUDE or EXCLUDE mode of one or more multicast groups.
 - Source list change record (unsolicited)—Sent by a host to change information about multicast sources.

Source-Based Filtering

MLD uses source-based filtering, which enables hosts and routers to specify which multicast sources should be allowed or blocked for a specific multicast group. Source-based filtering either allows or blocks traffic based on the following information in MLD messages:

- Source lists
- INCLUDE or EXCLUDE mode

Because the Layer 2 table is (MAC-group, VLAN) based, with MLD hosts it is preferable to have only a single multicast source per MAC-group.

**Note**

Source-based filtering is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection.

Explicit Host Tracking

MLD supports explicit tracking of membership information on any port. The explicit-tracking database is used for fast-leave processing, proxy reporting, and statistics collection. When explicit tracking is enabled on a VLAN, the MLD snooping software processes the MLD report it receives from a host and builds an explicit-tracking database that contains the following information:

- The port connected to the host
- The channels reported by the host
- The filter mode for each group reported by the host
- The list of sources for each group reported by the hosts
- The router filter mode of each group
- For each group, the list of hosts requesting the source

**Note**

- Disabling explicit host tracking disables fast-leave processing and proxy reporting.
- When explicit tracking is enabled and the switch is in report-suppression mode, the multicast router might not be able to track all the hosts accessed through a VLAN interface.

MLD Snooping Proxy Reporting

Because MLD does not have report suppression, all the hosts send their complete multicast group membership information to the multicast router in response to queries. The switch snoops these responses, updates the database and forwards the reports to the multicast router. To prevent the multicast router from becoming overloaded with reports, MLD snooping does proxy reporting.

Proxy reporting forwards only the first report for a multicast group to the router and suppresses all other reports for the same multicast group.

Proxy reporting processes solicited and unsolicited reports. Proxy reporting is enabled and cannot be disabled.

**Note**

Disabling explicit host tracking disables fast-leave processing and proxy reporting.

Joining an IPv6 Multicast Group

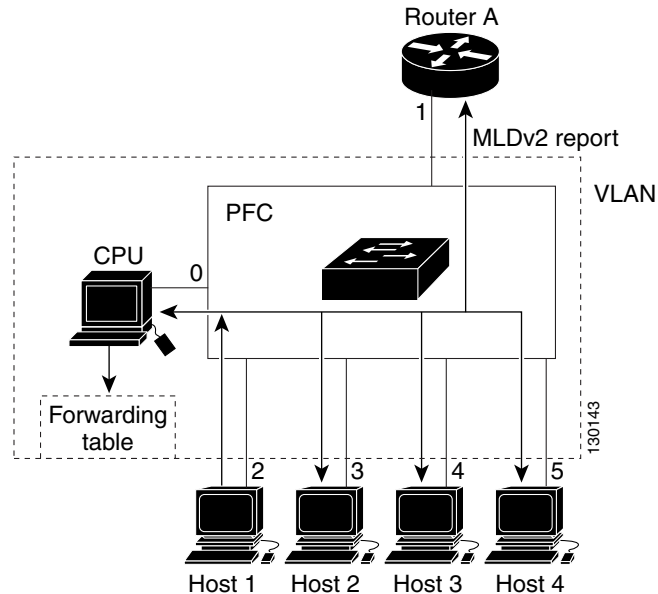
Hosts join IPv6 multicast groups either by sending an unsolicited MLD report or by sending an MLD report in response to a general query from an IPv6 multicast router (the switch forwards general queries from IPv6 multicast routers to all ports in a VLAN). The switch snoops these reports.

In response to a snooped MLD report, the switch creates an entry in its Layer 2 forwarding table for the VLAN on which the report was received. When other hosts that are interested in this multicast traffic send MLD reports, the switch snoops their reports and adds them to the existing Layer 2 forwarding table entry. The switch creates only one entry per VLAN in the Layer 2 forwarding table for each multicast group for which it snoops an MLD report.

MLD snooping suppresses all but one of the host reports per multicast group and forwards this one report to the IPv6 multicast router.

The switch forwards multicast traffic for the multicast group specified in the report to the interfaces where reports were received (see [Figure 36-1](#)).

Layer 2 multicast groups learned through MLD snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **mac-address-table static** command. When you specify group membership for a multicast group address statically, the static setting supersedes any MLD snooping learning. Multicast group membership lists can consist of both static and MLD snooping-learned settings.

Figure 36-1 Initial MLD Listener Report

Multicast router A sends an MLD general query to the switch, which forwards the query to ports 2 through 5 (all members of the same VLAN). Host 1 wants to join an IPv6 multicast group and multicasts an MLD report to the group with the equivalent MAC destination address of 0x0100.5E01.0203. When the switch snoops the MLD report multicast by Host 1, the switch uses the information in the MLD report to create a forwarding-table entry. [Table 36-1](#) shows the forwarding table, which includes the port numbers of Host 1, the multicast router, and the switch.

Table 36-1 MLD Snooping Forwarding Table

Destination MAC Address	Type of Packet	Ports
0100.5exx.xxxx	MLD	0
0100.5e01.0203	!MLD	1, 2

The switch hardware can distinguish MLD information packets from other packets for the multicast group. The first entry in the table indicates that only MLD packets should be sent to the CPU, which prevents the switch from becoming overloaded with multicast frames. The second entry indicates that frames addressed to the 0x0100.5E01.0203 multicast MAC address that are not MLD packets (!MLD) should be sent to the multicast router and to the host that has joined the group.

If another host (for example, Host 4) sends an unsolicited MLD report for the same group ([Figure 36-2](#)), the switch snoops that message and adds the port number of Host 4 to the forwarding table as shown in [Table 36-2](#). Because the forwarding table directs MLD messages only to the switch, the message is not flooded to other ports. Any known multicast traffic is forwarded to the group and not to the switch.

Figure 36-2 Second Host Joining a Multicast Group

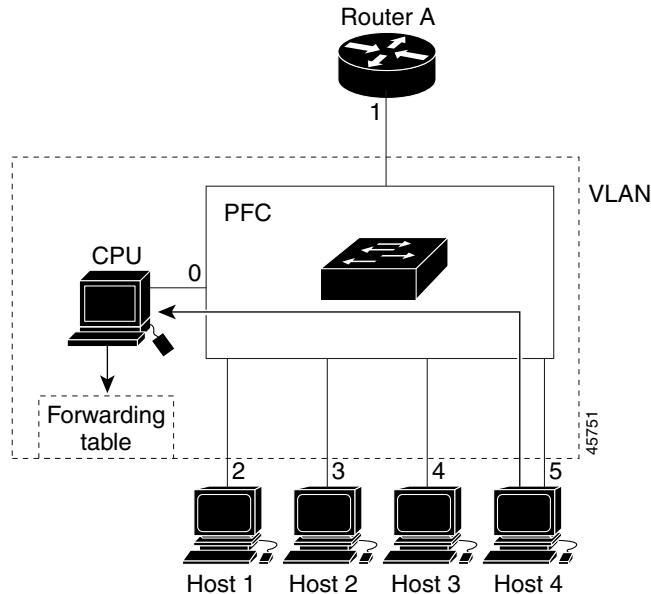


Table 36-2 Updated MLD Snooping Forwarding Table

Destination MAC Address	Type of Packet	Ports
0100.5exx.xxxx	MLD	0
0100.5e01.0203	!MLD	1, 2, 5

Leaving a Multicast Group

These sections describe leaving a multicast group:

- [Normal Leave Processing, page 36-6](#)
- [Fast-Leave Processing, page 36-7](#)

Normal Leave Processing

Interested hosts must continue to respond to the periodic MLD general queries. As long as at least one host in the VLAN responds to the periodic MLD general queries, the multicast router continues forwarding the multicast traffic to the VLAN. When hosts want to leave a multicast group, they can either ignore the periodic MLD general queries (called a “silent leave”), or they can send an MLD filter mode change record.

When MLD snooping receives a filter mode change record from a host that configures the EXCLUDE mode for a group, MLD snooping sends out a MAC-addressed general query to determine if any other hosts connected to that interface are interested in traffic for the specified multicast group.

If MLD snooping does not receive an MLD report in response to the general query, MLD snooping assumes that no other hosts connected to the interface are interested in receiving traffic for the specified multicast group, and MLD snooping removes the interface from its Layer 2 forwarding table entry for the specified multicast group.

If the filter mode change record was from the only remaining interface with hosts interested in the group, and MLD snooping does not receive an MLD report in response to the general query, MLD snooping removes the group entry and relays the MLD filter mode change record to the multicast router. If the multicast router receives no reports from a VLAN, the multicast router removes the group for the VLAN from its MLD cache.

The interval for which the switch waits before updating the table entry is called the “last member query interval.” To configure the interval, enter the **ipv6 mld snooping last-member-query-interval** *interval* command.

Fast-Leave Processing

Fast-leave processing is enabled by default. To disable fast-leave processing, turn off explicit-host tracking.

Fast-leave processing is implemented by maintaining source-group based membership information in software while also allocating LTL indexes on a MAC GDA basis.

When fast-leave processing is enabled, hosts send `BLOCK_OLD_SOURCES{src-list}` messages for a specific group when they no longer want to receive traffic from that source. When the switch receives such a message from a host, it parses the list of sources for that host for the given group. If this source list is exactly the same as the source list received in the leave message, the switch removes the host from the LTL index and stops forwarding this multicast group traffic to this host.

If the source lists do not match, the switch does not remove the host from the LTL index until the host is no longer interested in receiving traffic from any source.



Note

Disabling explicit host tracking disables fast-leave processing and proxy reporting.

Understanding the MLD Snooping Querier

Use the MLD snooping querier to support MLD snooping in a VLAN where PIM and MLD are not configured because the multicast traffic does not need to be routed.

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 switch 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 switches in the VLAN, but for each VLAN that is connected to switches that use MLD to report interest in IP multicast traffic, you must configure at least one switch as the MLD snooping querier.

You can configure a switch to generate MLD queries on a VLAN regardless of whether or not IP multicast routing is enabled.

Default MLD Snooping Configuration

Table 36-3 shows the default MLD snooping configuration.

Table 36-3 MLD Snooping Default Configuration

Feature	Default Values
MLD snooping querier	Disabled
MLD snooping	Enabled
Multicast routers	None configured
MLD report suppression	Enabled
MLD snooping router learning method	Learned automatically through PIM or MLD packets
Fast-Leave Processing	Enabled
MLD Explicit Host Tracking	Enabled

MLD Snooping Configuration Guidelines and Restrictions

When configuring MLD snooping, follow these guidelines and restrictions:

- Only PFC3C and PFC3CXL modes support MLD version 1 (MLDv1) and MLD version 2 (MLDv2).
- These modes support only MLD version 2 (MLDv2):
 - PFC3A
 - PFC3B
 - PFC3BXL
- MLD is derived from Internet Group Management Protocol version 3 (IGMPv3). MLD protocol operations and state transitions, host and router behavior, query and report message processing, message forwarding rules, and timer operations are exactly same as IGMPv3. See draft-vida-ml-d-02.txt for detailed information on MLD protocol.
- MLD protocol messages are Internet Control Message Protocol version 6 (ICMPv6) messages.
- MLD message formats are almost identical to IGMPv3 messages.
- IPv6 multicast for Cisco IOS software uses MLD version 2. This version of MLD is fully backward-compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 interoperate with a router running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are supported.
- MLD snooping supports private VLANs. Private VLANs do not impose any restrictions on MLD snooping.
- MLD snooping constrains traffic in MAC multicast groups 0100.5e00.0001 to 0100.5eff.ffff.
- MLD snooping does not constrain Layer 2 multicasts generated by routing protocols.

MLD Snooping Querier Configuration Guidelines and Restrictions

When configuring the MLD snooping querier, follow these guidelines and restrictions:

- Configure the VLAN in global configuration mode (see [Chapter 23, “Configuring VLANs”](#)).
- Configure an IPv6 address on the VLAN interface (see [Chapter 30, “Configuring Layer 3 Interfaces”](#)). When enabled, the MLD snooping querier uses the IPv6 address as the query source address.
- If there is no IPv6 address configured on the VLAN interface, the MLD snooping querier does not start. The MLD snooping querier disables itself if the IPv6 address is cleared. When enabled, the MLD snooping querier restarts if you configure an IPv6 address.
- When enabled, the MLD snooping querier does not start if it detects MLD traffic from an IPv6 multicast router.
- When enabled, the MLD snooping querier starts after 60 seconds with no MLD traffic detected from an IPv6 multicast router.
- When enabled, the MLD snooping querier disables itself if it detects MLD traffic from an IPv6 multicast router.
- QoS does not support MLD packets when MLD snooping is enabled.
- You can enable the MLD snooping querier on all the switches in the VLAN that support it. One switch is elected as the querier.

Enabling the MLD Snooping Querier

Use the MLD snooping querier to support MLD snooping in a VLAN where PIM and MLD are not configured because the multicast traffic does not need to be routed.

To enable the MLD snooping querier in a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# interface <i>vlan</i> <i>vlan_ID</i>	Selects the VLAN interface.
Step 2	Router(config-if)# ipv6 address <i>prefix/prefix_length</i>	Configures the IPv6 address and subnet.
Step 3	Router(config-if)# ipv6 mld snooping querier	Enables the MLD snooping querier.
	Router(config-if)# no ipv6 mld snooping querier	Disables the MLD snooping querier.
Step 4	Router(config-if)# end	Exits configuration mode.
Step 5	Router# show ipv6 mld interface <i>vlan</i> <i>vlan_ID</i> include querier	Verifies the configuration.

This example shows how to enable the MLD snooping querier on VLAN 200 and verify the configuration:

```
Router# interface vlan 200
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
Router(config-if)# ipv6 mld snooping querier
Router(config-if)# end
Router# show ipv6 mld interface vlan 200 | include querier
      MLD snooping fast-leave is enabled and querier is enabled
```

Configuring MLD Snooping


Note

To use MLD snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLD snooping querier in the subnet (see the “[Enabling the MLD Snooping Querier](#)” section on page 36-9).

These sections describe how to configure MLD snooping:

- [Enabling MLD Snooping](#), page 36-10
- [Configuring a Static Connection to a Multicast Receiver](#), page 36-11
- [Enabling Fast-Leave Processing](#), page 36-13
- [Configuring Explicit Host Tracking](#), page 36-13
- [Configuring Report Suppression](#), page 36-14
- [Displaying MLD Snooping Information](#), page 36-14


Note

Except for the global enable command, all MLD snooping commands are supported only on VLAN interfaces.

Enabling MLD Snooping

To enable MLD snooping globally, perform this task:

	Command	Purpose
Step 1	Router(config)# ipv6 mld snooping	Enables MLD snooping.
	Router(config)# no ipv6 mld snooping	Disables MLD snooping.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show ipv6 mld interface vlan vlan_ID include globally	Verifies the configuration.

This example shows how to enable MLD snooping globally and verify the configuration:

```
Router(config)# ipv6 mld snooping
Router(config)# end
Router# show ipv6 mld interface vlan 200 | include globally
  MLD snooping is globally enabled
Router#
```

To enable MLD snooping in a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan vlan_ID	Selects a VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping	Enables MLD snooping.
	Router(config-if)# no ipv6 mld snooping	Disables MLD snooping.

	Command	Purpose
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show ipv6 mld interface vlan <i>vlan_ID</i> include snooping	Verifies the configuration.

This example shows how to enable MLD snooping on VLAN 25 and verify the configuration:

```
Router# interface vlan 25
Router(config-if)# ipv6 mld snooping
Router(config-if)# end
Router# show ipv6 mld interface vlan 25 | include snooping
MLD snooping is globally enabled
MLD snooping is enabled on this interface
MLD snooping fast-leave is enabled and querier is enabled
MLD snooping explicit-tracking is enabled
MLD snooping last member query response interval is 1000 ms
MLD snooping report-suppression is disabled
Router#
```



Note

For WS-SUP720-3B, the maximum threshold value for MLD snooping is 32000 entries. With MLD snooping enabled, surpassing this threshold might lead to a crash. Disabling MLD snooping will allow the switch to process larger number of entries.

Configuring a Static Connection to a Multicast Receiver

To configure a static connection to a multicast receiver, perform this task:

	Command	Purpose
Step 1	Router(config)# mac-address-table static <i>mac_addr</i> vlan <i>vlan_id</i> interface <i>type</i>¹ <i>slot/port</i> [disable-snooping]	Configures a static connection to a multicast receiver.
Step 2	Router(config-if)# end	Exits configuration mode.
Step 3	Router# show mac-address-table address <i>mac_addr</i>	Verifies the configuration.

- ¹ *type* = fastethernet, gigabitethernet, or tengigabitethernet

When you configure a static connection, enter the **disable-snooping** keyword to prevent multicast traffic addressed to the statically configured multicast MAC address from also being sent to other ports in the same VLAN.

This example shows how to configure a static connection to a multicast receiver:

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 interface fastethernet 5/7
```

Configuring a Multicast Router Port Statically

To configure a static connection to a multicast router, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects the VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping mrouter interface <i>type</i> ¹ <i>slot/port</i>	Configures a static connection to a multicast router.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show ipv6 mld snooping mrouter	Verifies the configuration.

1. *type* = fastethernet, gigabitethernet, or tengigabitethernet

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

This example shows how to configure a static connection to a multicast router:

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

Configuring the MLD Snooping Query Interval

You can configure the interval for which the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group.



Note

When both MLD snooping fast-leave processing and the MLD snooping query interval are configured, fast-leave processing takes precedence.

To configure the interval for the MLD snooping queries sent by the switch, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping last-member-query-interval <i>interval</i>	Configures the interval for the IGMP queries sent by the switch. Default is 1 second. Valid range is 1000 to 9990 milliseconds.
Step 3	Router# show ipv6 mld interface vlan <i>vlan_ID</i> include last	Verifies the configuration.

This example shows how to configure the MLD snooping query interval:

```
Router(config-if)# ipv6 mld snooping last-member-query-interval 1000
Router(config-if)# exit
Router# show ipv6 mld interface vlan 200 | include last
MLD snooping last member query response interval is 1000 ms
```

Enabling Fast-Leave Processing

To enable fast-leave processing in a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping fast-leave	Enables fast-leave processing in the VLAN.
Step 3	Router# show ipv6 mld interface vlan <i>vlan_ID</i> include fast-leave	Verifies the configuration.

This example shows how to enable fast-leave processing on the VLAN 200 interface and verify the configuration:

```
Router# interface vlan 200
Router(config-if)# ipv6 mld snooping fast-leave
Configuring fast leave on vlan 200
Router(config-if)# end
Router# show ipv6 mld interface vlan 200 | include fast-leave
      MLD snooping fast-leave is enabled and querier is enabled
Router#
```

Enabling SSM Safe Reporting

To enable source-specific multicast (SSM) safe reporting, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping ssm-safe-reporting	Enables SSM safe reporting.
	Router(config-if)# no ipv6 mld snooping ssm-safe-reporting	Clears the configuration.

This example shows how to SSM safe reporting:

```
Router(config)# interface vlan 10
Router(config-if)# ipv6 mld snooping ssm-safe-reporting
```

Configuring Explicit Host Tracking



Note

Disabling explicit host tracking disables fast-leave processing and proxy reporting.

To enable explicit host tracking on a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
	Router(config-if)# no ipv6 mld snooping explicit-tracking	Clears the explicit host tracking configuration.
Step 3	Router# show ipv6 mld snooping explicit-tracking vlan <i>vlan_ID</i>	Displays the status of explicit host tracking.

This example shows how to enable explicit host tracking:

```
Router(config)# interface vlan 25
Router(config-if)# ipv6 mld snooping explicit-tracking
Router(config-if)# end
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group          Interface    Reporter    Filter_mode
-----
10.1.1.1/226.2.2.2    V125:1/2    16.27.2.3    INCLUDE
10.2.2.2/226.2.2.2    V125:1/2    16.27.2.3    INCLUDE
```

Configuring Report Suppression

To enable report suppression on a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2	Router(config-if)# ipv6 mld snooping report-suppression	Enables report suppression.
	Router(config-if)# no ipv6 mld snooping report-suppression	Clears the report suppression configuration.
Step 3	Router# show ipv6 mld interface <i>vlan_ID</i> include report-suppression	Displays the status of report suppression.

This example shows how to enable explicit host tracking:

```
Router(config)# interface vlan 25
Router(config-if)# ipv6 mld snooping report-suppression
Router(config-if)# end
Router# Router# show ipv6 mld interface vlan 25 | include report-suppression
MLD snooping report-suppression is enabled
```

Displaying MLD Snooping Information

These sections describe displaying MLD snooping information:

- [Displaying Multicast Router Interfaces, page 36-15](#)
- [Displaying MAC Address Multicast Entries, page 36-15](#)
- [Displaying MLD Snooping Information for a VLAN Interface, page 36-15](#)

Displaying Multicast Router Interfaces

When you enable IGMP snooping, the switch automatically learns to which interface the multicast routers are connected.

To display multicast router interfaces, perform this task:

Command	Purpose
Router# show ipv6 mld snooping mrouter <i>vlan_ID</i>	Displays multicast router interfaces.

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan          ports
-----+-----
  1           Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

Displaying MAC Address Multicast Entries

To display MAC address multicast entries for a VLAN, perform this task:

Command	Purpose
Router# show mac-address-table multicast <i>vlan_ID</i> [<i>count</i>]	Displays MAC address multicast entries for a VLAN.

This example shows how to display MAC address multicast entries for VLAN 1:

```
Router# show mac-address-table multicast vlan 1
vlan  mac address      type    qos      ports
-----+-----+-----+-----+-----
  1   0100.5e02.0203  static  --   Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0127  static  --   Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0128  static  --   Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0001  static  --   Gi1/1,Gi2/1,Fa3/48,Router,Switch
Router#
```

This example shows how to display a total count of MAC address entries for a VLAN:

```
Router# show mac-address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

Displaying MLD Snooping Information for a VLAN Interface



Note

When you apply the **ipv6 mld snooping** command and associated commands on any VLAN interface, the commands continue to function even if the VLAN interface is in shutdown state.

To display MLD snooping information for a VLAN interface, perform this task:

Command	Purpose
Router# show ipv6 mld snooping { explicit-tracking <i>vlan_ID</i> } { mrouter [vlan <i>vlan_ID</i>]} { report-suppression vlan <i>vlan_ID</i> } { statistics vlan <i>vlan_ID</i> }	Displays MLD snooping information on a VLAN interface.

This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group          Interface    Reporter    Filter_mode
-----
10.1.1.1/226.2.2.2    V125:1/2    16.27.2.3    INCLUDE
10.2.2.2/226.2.2.2    V125:1/2    16.27.2.3    INCLUDE
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan          ports
-----
1             Gi1/1,Gi2/1,Fa3/48,Router
```

This example shows IGMP snooping statistics information for VLAN 25:

```
Router# show ipv6 mld snooping statistics interface vlan 25

Snooping staticstics for Vlan25
#channels:2
#hosts    :1

Source/Group          Interface    Reporter    Uptime      Last-Join    Last-Leave
-----
10.1.1.1/226.2.2.2    Gi1/2:V125    16.27.2.3    00:01:47    00:00:50    -
10.2.2.2/226.2.2.2    Gi1/2:V125    16.27.2.3    00:01:47    00:00:50    -
```



Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[Participate in the Technical Documentation Ideas forum](#)