IPv6 Multicast Listener Discovery Protocol

- Restrictions for IPv6 Multicast Listener Discovery Protocol, on page 1
- Information About IPv6 Multicast Listener Discovery Protocol, on page 1
- How to Configure IPv6 Multicast Listener Discovery Protocol, on page 4
- Verifying IPv6 Multicast Listener Discovery Protocol, on page 10

Restrictions for IPv6 Multicast Listener Discovery Protocol

- MLD snooping is not supported. IPv6 multicast traffic is flooded to all Ethernet Flow Points (EFPs) or Trunk EFPs (TEFPs) associated with a bridge domain.
- MLD proxy is not supported.
- For RSP1A, more than 1000 IPv6 multicast routes are not supported.
- For RSP1B, more than 2000 IPv6 multicast routes are not supported.
- IPv6 Multicast Listener Discovery protocol is *not* supported on the ASR 900 RSP3 module.

Information About IPv6 Multicast Listener Discovery Protocol

IPv6 Multicast Overview

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries; receivers can be located anywhere on the Internet or in any private network. Receivers that are interested in receiving data flowing to a particular group must join the group by signaling their local device. This signaling is achieved with the MLD protocol.

Devices use the MLD protocol to learn whether or not members of a group are present on their directly attached subnets. Hosts join multicast groups by sending MLD report messages. The network then delivers data to a potentially unlimited number of receivers, using only one copy of the multicast data on each subnet. IPv6 hosts that wish to receive the traffic are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast packets.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

A multicast address is chosen for the receivers in a multicast group. Senders use this address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

How active a multicast group is, its duration, and its membership can vary from group to group and from time to time. A group that has members may have no activity.

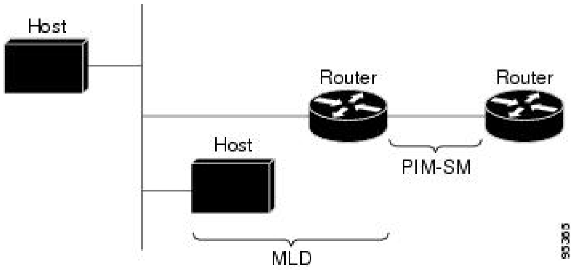
IPv6 Multicast Routing Implementation

Cisco software supports the following protocols to implement IPv6 multicast routing:

- MLD is used by IPv6 devices to discover multicast listeners on directly attached links. There are two versions of MLD:
  - MLD version 1 is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.
  - MLD version 2 is based on version 3 of the IGMP for IPv4.
- IPv6 multicast for Cisco software uses both MLD version 2 and MLD version 1. MLD version 2 is fully backward-compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 interoperate with a device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM-SM is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in Source Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address.

The figure below shows where MLD and PIM-SM operate within the IPv6 multicast environment.

Figure 1: IPv6 Multicast Routing Protocols Supported for IPv6



Multicast Listener Discovery Protocol for IPv6

To start implementing multicasting in the campus network, users must first define who receives the multicast. The MLD protocol is used by IPv6 devices to discover the presence of multicast listeners (for example, nodes that want to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. It is used for discovering local group and source-specific group membership. The MLD protocol provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

The difference between multicast queriers and hosts is as follows:

- A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver that sends report messages to inform the querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use MLD reports to join and leave multicast groups and to begin receiving group traffic.

MLD uses the Internet Control Message Protocol (ICMP) to carry its messages. All MLD messages are link-local with a hop limit of 1, and they all have the alert option set. The alert option implies an implementation of the hop-by-hop option header.

MLD has three types of messages:

- Query—General, group-specific, and multicast-address-specific. In a query message, the multicast address field is set to 0 when MLD sends a general query. The general query learns which multicast addresses have listeners on an attached link.

Note Group-specific and multicast-address-specific queries are the same. A group address is a multicast address.

- Report—In a report message, the multicast address field is that of the specific IPv6 multicast address to which the sender is listening.
- Done—In a done message, the multicast address field is that of the specific IPv6 multicast address to which the source of the MLD message is no longer listening.

An MLD report must be sent with a valid IPv6 link-local source address, or the unspecified address (::), if the sending interface has not yet acquired a valid link-local address. Sending reports with the unspecified address is allowed to support the use of IPv6 multicast in the Neighbor Discovery Protocol.

For stateless autoconfiguration, a node is required to join several IPv6 multicast groups in order to perform duplicate address detection (DAD). Prior to DAD, the only address the reporting node has for the sending interface is a tentative one, which cannot be used for communication. Therefore, the unspecified address must be used.

MLD states that result from MLD version 2 or MLD version 1 membership reports can be limited globally or by interface. The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets. Membership reports in excess of the configured limits is not entered in the MLD cache, and traffic for those excess membership reports will not be forwarded.

MLD provides support for source filtering. Source filtering allows a node to report interest in listening to packets only from specific source addresses (as required to support SSM), or from all addresses except specific source addresses sent to a particular multicast address.

When a host using MLD version 1 sends a leave message, the device needs to send query messages to reconfirm that this host was the last MLD version 1 host joined to the group before it can stop forwarding traffic. This function takes about 2 seconds. This "leave latency" is also present in IGMP version 2 for IPv4 multicast.

MLD Access Group

MLD access groups provide receiver access control in Cisco IPv6 multicast devices. This feature limits the list of groups a receiver can join, and it allows or denies sources used to join SSM channels.

How to Configure IPv6 Multicast Listener Discovery Protocol

Enabling IPv6 Multicast Routing

To enable IPv6 multicast routing, complete the following steps:

Before you begin

You must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing.

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	**ipv6 multicast-routing** [**vrf** *vrf-name*] **Example:** `Device(config)# ipv6 multicast-routing`	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device. IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. On certain devices, the IPv6 multicast routing must also be enabled in order to use IPv6 unicast routing. • vrf *vrf-name*—(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits to privileged EXEC mode.

Customizing MLD on an Interface

To customize MLD on an interface, complete the following steps:

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	**ipv6 mld state-limit** *number* **Example:** `Device(config)# ipv6 mld state-limit 300`	Configures a limit on the number of MLD states resulting from MLD membership reports on a global basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache and traffic for the excess membership reports is not forwarded. • *number*—Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.
Step 4	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable** **Example:** `Device(config)# ipv6 mld ssm-map enable`	Enables the Source Specific Multicast (SSM) mapping feature for groups in the configured SSM range. • vrf *vrf-name*— (Optional) Specifies a virtual routing and forwarding (VRF) configuration.
Step 5	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 1/0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 6	**ipv6 mld access-group** *access-list-name* **Example:** `Device(config-if)# ipv6 access-list acc-grp-1`	Allows the user to perform IPv6 multicast receiver access control. • *access-list-name*—A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

	Command or Action	Purpose

Step 7	**ipv6 mld static-group** [*group-address*] [[**include**| **exclude**] {*source-address* | **source-list** [*acl*]}
	Example:
	`Device(config-if)# ipv6 mld static-group ff04::10 include 100::1`
		Statically forwards traffic for the multicast group onto a specified interface and cause the interface to behave as if a MLD joiner were present on the interface.
		• *group-address*—(Optional) IPv6 address of the multicast group.
		• include—(Optional) Enables include mode.
		• exclude—(Optional) Enables exclude mode.
		• *source-address*—Unicast source address to include or exclude.
		• source-list—Source list on which MLD reporting is to be configured.
		• *acl*—(Optional) Access list used to include or exclude multiple sources for the same group.

Step 8	**ipv6 mld query-max-response-time** *seconds* **Example:** `Device(config-if)# ipv6 mld query-max-response-time 20`	Configures the maximum response time advertised in MLD queries. • *seconds*—Maximum response time, in seconds, advertised in MLD queries. The default value is 10 seconds.
Step 9	**ipv6 mld query-timeout** *seconds* **Example:** `Device(config-if)# ipv6 mld query-timeout 130`	Configures the timeout value before the device takes over as the querier for the interface. • *seconds*—Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier.
Step 10	**ipv6 mld query-interval** *seconds* **Example:** `Device(config-if)# ipv6 mld query-interval 60`	Configures the frequency at which the Cisco IOS XE software sends MLD host-query messages. • *seconds*—Frequency, in seconds, at which to send MLD host-query messages. It can be a number from 0 to 65535. The default is 125 seconds. **Caution** Changing this value may severely impact multicast forwarding.

	Command or Action	Purpose
Step 11	**ipv6 mld limit** *number* [**except** *access-list*] **Example:** `Device(config-if)# ipv6 mld limit 100`	Configures a limit on the number of MLD states resulting from MLD membership reports on a per-interface basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache, and traffic for the excess membership reports is not forwarded. Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state is ignored if it exceeds either the per-interface limit or global limit. If you do not configure the except *access-list* keyword and argument, all MLD states are counted toward the configured cache limit on an interface. Use the except *access-list* keyword and argument to exclude particular groups or channels from counting toward the MLD cache limit. An MLD membership report is counted against the per-interface limit if it is permitted by the extended access list specified by the except *access-list* keyword and argument. • *number*—Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000. • except—(Optional) Excludes an access list from the configured MLD state limit. • *access-list*—(Optional) Access list to exclude from the configured MLD state limit.

Step 12	**end**
	Example:
	`Device(config-if)# end`
		Exits to privileged EXEC mode.

Disabling MLD Device-Side Processing

A user might only want specified interfaces to perform IPv6 multicast and therefore want to turn off MLD device-side processing on a specified interface. To disable MLD device-side processing, complete the following steps:

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	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 1/0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**no ipv6 mld router** **Example:** `Device(config-if)# no ipv6 mld router`	Disables MLD device-side processing on a specified interface.

Resetting the MLD Traffic Counters

To reset the MLD traffic counters, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 mld** [**vrf** *vrf-name*] **traffic** **Example:** `Device# clear ipv6 mld traffic`	Resets all MLD traffic counters. • **vrf** *vrf-name*—(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Clearing the MLD Interface Counters

To clear the MLD interface counters, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 mld** [**vrf** *vrf-name*] **counters** *interface-type* **Example:** `Device# clear ipv6 mld counters GigabitEthernet1/0/0`	Clears the MLD interface counters. • vrf *vrf-name*—(Optional) Specifies a virtual routing and forwarding (VRF) configuration. • *interface-type*—(Optional) Interface type. For more information, use the question mark (?) online help function.

Clearing the MLD Groups

To clear MLD related information in the IPv6 multicast routing table, complete the following steps:

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	**clear ipv6** [**icmp**] **mld groups** {* | *group-prefix* | *group* [*source*]} [**vrf** {*vrf-name* | **all**}] **Example:** `Device (config)# clear ipv6 mld groups *`	Clears the MLD groups information. • icmp—(Optional) Clears ICMP information. • *— Specifies all routes. • *group-prefix*—Group prefix. • *group*—Group address. • *source*—(Optional) Source (S, G) route. • vrf—(Optional) Applies to a virtual routing and forwarding (VRF) instance.

	Command or Action	Purpose
		- *vrf-name*—(Optional) VRF name. The name can be alphanumeric, case sensitive, or a maximum of 32 characters. - all—Specifies all VRFs.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits to privileged EXEC mode.

Verifying IPv6 Multicast Listener Discovery Protocol

- Use the **show ipv6 mld groups** [**link-local**] [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] command to display the multicast groups that are directly connected to the device and that were learned through MLD:

```
Router# show ipv6 mld groups
```

```
MLD Connected Group Membership
Group Address                           Interface          Uptime    Expires
FF08::1                                Gi0/4/4            00:10:22  00:04:19
```

- Use the **show ipv6 mfib** [**vrf** *vrf-name*] [**all** | **linkscope** | **verbose** | *group-address-name* | *ipv6-prefix/prefix-length* | *source-address-name* | **interface** | **status** | **summary**] command display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB).

  The following example shows forwarding entries and interfaces in the MFIB specified with a group address of FF08:1::1:

```
Router# show ipv6 mfib ff08::1
```

```
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
               A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,

                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,FF08::1) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 264/264/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   Tunnel1 Flags: A NS
   GigabitEthernet0/4/4 Flags: F NS
     Pkts: 0/0
 (2000::8,FF08::1) Flags: HW
   SW Forwarding: 1/0/132/0, Other: 0/0/0
   HW Forwarding:   75852/1047/150/1226, Other: 0/0/0
   GigabitEthernet0/4/2 Flags: A
   GigabitEthernet0/4/4 Flags: F NS
     Pkts: 0/1
```

- Use the **show ipv6 mld interface** [*type number*] command to display multicast-related information about an interface.

  The following is sample output from the **show ipv6 mld interface** command for Gigabit Ethernet interface 0/4/4:

  ```
  Router# show ipv6 mld interface gigabitethernet 0/4/4
  ```

  ```
  GigabitEthernet0/4/4 is up, line protocol is up
    Internet address is FE80::D2C2:82FF:FE17:77C4/10
    MLD is enabled on interface
    Current MLD version is 2
    MLD query interval is 125 seconds
    MLD querier timeout is 255 seconds
    MLD max query response time is 10 seconds
    Last member query response interval is 1 seconds
    MLD activity: 7 joins, 0 leaves
    MLD querying router is FE80::D2C2:82FF:FE17:77C4 (this system)
  ```

- Use the **show ipv6 mld** [**vrf** *vrf-name*] **traffic** command to display the MLD traffic counters:

  ```
  Router# show ipv6 mld traffic
  ```

  ```
  MLD Traffic Counters
  Elapsed time since counters cleared: 00:11:25

                                Received     Sent
  Valid MLD Packets               672         85
  Queries                         7           20
  Reports                         665         65
  Leaves                          0           0
  Mtrace packets                  0           0

  Errors:
  Malformed Packets                           0
  Martian source                              2
  Non link-local source                       0
  Hop limit is not equal to 1                 0
  ```

- Use the **show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]]] command to display the information in the PIM topology table:

  ```
  Router# show ipv6 mroute ff08::1
  ```

  ```
  Multicast Routing Table
  Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
         C - Connected, L - Local, I - Received Source Specific Host Report,
         P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
         J - Join SPT, Y - Joined MDT-data group,
         y - Sending to MDT-data group
         g - BGP signal originated, G - BGP Signal received,
         N - BGP Shared-Tree Prune received, n - BGP C-Mroute suppressed,
         q - BGP Src-Active originated, Q - BGP Src-Active received
         E - Extranet
  Timers: Uptime/Expires
  Interface state: Interface, State
  ```

```
(*, FF08::1), 00:11:18/never, RP 4000::1, flags: SCJ
  Incoming interface: Tunnel1
  RPF nbr: 4000::1
  Immediate Outgoing interface list:
    GigabitEthernet0/4/4, Forward, 00:11:18/never

(2000::8, FF08::1), 00:02:07/00:01:22, flags: SFJT
  Incoming interface: GigabitEthernet0/4/2
  RPF nbr: 2000::8
  Inherited Outgoing interface list:
    GigabitEthernet0/4/4, Forward, 00:11:18/never
```