IPv6 Multicast

This feature module describes how to configure basic IP multicast in an IPv6 network.

- Prerequisites for IPv6 Multicast, on page 1
- Restrictions for IPv6 Multicast, on page 1
- Information About IPv6 Multicast, on page 2
- Configuring IPv6 Multicast, on page 7
- Configuration Examples for IPv6 Multicast, on page 39
- Troubleshooting Tips, on page 42

Prerequisites for IPv6 Multicast

- Cisco IOS Release 15.4(1)S or a later release that supports the IPv6 Multicast feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- You must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing.

Restrictions for IPv6 Multicast

- PIM Dense Mode is not supported.
- Bidirectional Protocol Independent Multicast (PIM) is not supported.
- You must disable the Source Specific Multicast (SSM) map query dns when static mapping is configured.
- You must configure the **asr901-platf-multicast enable** command to enable multicast on the Cisco ASR 901 router.
- You must enable the **asr901-multicast source** command on the SVI interface that is connected to the traffic source.
- Mroute based counter or rate statistics are not supported. Multicast counters are not supported.
- Multicast VPN (MVPN) is not supported.
- PIM IPv6 SSM in VRF lite is supported only from Cisco IOS release 15.4(3)S.
- PIM IPv6 SM in VRF lite is not supported.
- IPv6 PIM interface counters are not supported till Cisco IOS Release 15.5(1)S.
- Multicast is *not* supported on Serial and MLPPP interfaces.

- Multiple L3 SVI interfaces on PoCH as replication VLAN's for multicast traffic are not supported.
- IP Multicast on loopback interface is not supported.

Information About IPv6 Multicast

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 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 that 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 Groups

An IPv6 address must be configured on an interface for the interface to forward IPv6 traffic. Configuring a site-local or global IPv6 address on an interface automatically configures a link-local address and activates IPv6 for that interface. Additionally, the configured interface automatically joins the following required multicast groups for that link:

- Solicited-node multicast group FF02:0:0:0:0:1:FF00::/104 for each unicast and anycast address assigned to the interface
- All-nodes link-local multicast group FF02::1
- All-routers link-local multicast group FF02::2

IPv6 Multicast Routing Implementation

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

- MLD for IPv6: MLD is used by IPv6 routers to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions of MLD:
    - MLD version 1 is based on version 2 of the IGMP for IPv4

  - MLD version 2 is based on version 3 of the IGMP for IPv4.

- IPv6 multicast for Cisco IOS 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 interoperates with a router running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in PIM SSM has 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.

Multicast Listener Discovery Protocol for IPv6

To start implementing multicasting in a 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 differences between multicast queriers and hosts are 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 send 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. 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 are not entered in the MLD cache, and traffic for those excess membership reports are not 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 Snooping

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes looking to receive IPv6 multicast packets) on its directly attached links, and to discover which multicast packets are of interest to neighboring nodes.

Using MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that looks to receive the data, instead of data being flooded to all the ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

For more information on MLD snooping, see the *IPv6 MLD Snooping* document at: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/ipv6_mld_snooping.html

MLD Snooping Support

IP address-based MLD snooping is enabled on the Cisco ASR 901 Routers with the following specifics:

- Source specific MLD snooping is not supported.
- When MLD snooping is configured, unknown multicast packets are flooded to the BD.

Layer 2 VPN on the Physical Interface

- Default and port-based Xconnet—MLD packets (control and data) are sent over an L2 VPN session.
- Dot1Q-based Xconnect—If Xconnect is configured for a customer VLAN, MLD packets (control and data) are carried into an L2 VPN. If they are not MLD control packets they are handled as reserved multicast packets in the BD VLAN, and data packets are forwarded according to the data in the MLD snooping tables.

Layer 3 IP Multicast with IP MLD Snooping

- Flows destined for PIM Sparse Mode-enabled and PIM Source-Specific Multicast-enabled groups are forwarded using Layer 3 IP multicast logic.
- Flows destined for groups that are populated using data in the MLD snooping table are forwarded using MLD snooping forward logic.
- Flows that are common (destined for groups that are populated using PIM-SM or PIM-SSM and MLD snooping):
    - The accept interface of PIM-SM or PIM-SSM Multicast Forwarding Information Base (MFIB) is the same as the BD VLAN in which MLD snooping-based forwarding takes place.
    - Layer 3 forwarding takes place using Layer 3 interface output of PIM-SM or PIM-SSM MFIB.

- Layer 2 forwarding takes place using the output ports from the MLD snooping logic.

The following are supported as part of MLD snooping:

- MLD message processing
- IPv6 MLD snooping
- Packet forwarding at hardware within bridge domain using IP multicast address lookup and IPv6 MLD information.

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs. PIM works independently of the unicast routing protocol to perform send or receive multicast route updates like other protocols. Regardless of which unicast routing protocols are being used in the LAN to populate the unicast routing table, Cisco IOS PIM uses the existing unicast table content to perform the Reverse Path Forwarding (RPF) check instead of building and maintaining its own separate routing table.

For more information on PIM, see the *IP Multicast Technology Overview* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/imc_tech_oview.html

PIM Source Specific Multicast

PIM SSM is the routing protocol that supports the implementation of SSM and is derived from PIM SM. However, unlike PIM SM where data from all multicast sources are sent when there is a PIM join, the SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, thus optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. Further, instead of the use of RP and shared trees, SSM uses information found on source addresses for a multicast group. This information is provided by receivers through the source addresses relayed to the last-hop devices by MLD membership reports, resulting in shortest-path trees directly to the sources.

In SSM, delivery of datagrams is based on the (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IPv6 unicast source address S and the multicast group address G as the IPv6 destination address. Systems receive this traffic by becoming members of the (S, G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources.

MLD version 2 is required for SSM to operate. MLD allows the host to provide source information. Before SSM runs with MLD, SSM must be supported in the Cisco IPv6 device, the host where the application is running, and the application itself.

For more information on PIM Source-Specific Multicast, see the *IP Multicast: PIM Configuration Guide* at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/ip6-mcast-pim-ssm.html

Source Specific Multicast Mapping for IPv6

SSM mapping for IPv6 supports both static and dynamic Domain Name System (DNS) mapping for MLD version 1 receivers. This feature allows deployment of IPv6 SSM with hosts that are incapable of providing MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application.

SSM mapping allows the device to look up the source of a multicast MLD version 1 report either in the running configuration of the device or from a DNS server. The device can then initiate an (S, G) join toward the source.

For more information on IPv6 Source Specific Multicast Mapping, see the *IP Multicast: PIM Configuration Guide* at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/ip6-mcast-ssm-map.html

PIM-Sparse Mode

PIM-SM uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data receive the traffic.

PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least, initially), it requires the use of a rendezvous point (RP). The RP must be administratively configured in the network.

For more information on PIM Sparse Mode, see the *IP Multicast: PIM Configuration Guide* at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/ip6-mcast-pim-sm.html

Rendezvous Point

A rendezvous point (RP) is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM). The protocol is described in RFC 2362.

For more information on RP, see the Configuring a Rendezvous Point guide at: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

The recommended methods for configuring an RP in a PIM-SM network are given below:

- Static RP
- Bootstrap router
- Anycast RP

IPv6 Multicast VRF Lite

The IPv6 Multicast VRF Lite feature provides IPv6 multicast support for multiple virtual routing/forwarding contexts (VRFs). The scope of these VRFs is limited to the router in which the VRFs are defined.

This feature provides separation between routing and forwarding, providing an additional level of security because no communication between devices belonging to different VRFs is allowed unless it is explicitly configured. The IPv6 Multicast VRF Lite feature simplifies the management and troubleshooting of traffic belonging to a specific VRF.

Note Only PIM SSM is supported, PIM SM is not supported in VRF Lite.

PIM BFD

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols and independent of the higher layer protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier and reconvergence time is consistent and predictable.

Protocol Independent Multicast (PIM) uses a hello mechanism for discovering new neighbors and for detecting failures between adjacent nodes. The minimum failure detection time in PIM is 3 times the PIM Query-Interval. To enable faster failure detection, the rate at which a PIM Hello message is transmitted on an interface is configurable. However, lower intervals increase the load on the protocol and can increase CPU and memory utilization and cause a system-wide negative impact on performance. Lower intervals can also cause PIM neighbors to expire frequently as the neighbor expiry can occur before the hello messages received from those neighbors are processed.

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD to initiate a session with an adjacent PIM node to support BFD's fast adjacency failure detection in the protocol layer. PIM registers just once for both PIM and IPv6 PIM.

At PIMs request (as a BFD client), BFD establishes and maintains a session with an adjacent node for maintaining liveness and detecting forwarding path failure to the adjacent node. PIM hellos will continue to be exchanged between the neighbors even after BFD establishes and maintains a BFD session with the neighbor. The behavior of the PIM hello mechanism is not altered due to the introduction of this feature.

Although PIM depends on the Interior Gateway Protocol (IGP) and BFD is supported in IGP, PIM BFD is independent of IGP's BFD.

Configuring IPv6 Multicast

Enabling IPv6 Multicast Routing

To enable IPv6 Multicast Routing feature, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ipv6 multicast-routing** *[***vrf** *vrf-name]* **Example:** `Router(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.
Step 4	**asr901-platf-multicast enable** **Example:** `Router(config)# asr901-platf-multicast enable`	Enables the platform multicast routing.

Disabling IPv6 Multicast Forwarding

This procedure disables IPv6 multicast forwarding on the router. The IPv6 multicast forwarding is turned on by default when IPv6 multicast routing is enabled.

To disable IPv6 multicast forwarding, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**no ipv6 mfib** **Example:** `Router(config)# no ipv6 mfib`	Disables IPv6 multicast forwarding on the router.

Disabling MLD Device-Side Processing

MLD is enabled on every interface when IPv6 multicast routing is configured. This procedure disables MLD router side processing on that interface. The router stops sending MLD queries and stops keeping track of MLD members on the LAN. If the **ipv6 mld join-group** command is configured on this interface, the interface continues with the MLD host functionality and report group membership when MLD query is received.

To turn off MLD device-side processing on a specified interface, complete the following steps:

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 105`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**no ipv6 mld router** **Example:** `Router(config)# no ipv6 mld router`	Disables MLD device-side processing on a specified interface.

Configuring MLD Protocol on an Interface

To configure Multicast Listener Discovery Protocol on an interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 104`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 mld query-interval** *seconds* **Example:** **Example:** `Router(config-if)# ipv6 mld query-interval 60`	Configures the frequency of MLD Host-Query packets transmitted. A designated router for a LAN is the only router that transmits queries. The default value is 60 seconds.
Step 5	**ipv6 mld query-max-response-time** *seconds* **Example:** `Router(config-if)# ipv6 mld query-max-response-time 20`	Specifies the maximum query response time advertised in the MLD queries. Default value is 10 seconds. Configuring a value less than 10 seconds enables the router to prune groups faster.

	Command or Action	Purpose
Step 6	**ipv6 mld query-timeout** *seconds* **Example:** `Router(config-if)# ipv6 mld query-timeout 130`	Specifies the timeout for the router to take over as the querier for the interface, after the previous querier has stopped querying. The default value is 2 * query-interval. If the router hears no queries for the timeout period, it becomes the querier.

Step 7	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]}
	Example:
	`Router(config-if)# ipv6 mld join-group ff04::12 exclude 2001:DB8::10:11`
		Configures MLD reporting for given *group* with MLDv1 or given *source* and *group* with MLDv2. The packets that are addressed to this group address are passed up to the client process in the router as well forwarded out the interface.

Step 8	**ipv6 mld static-group** [*group-address*] [**include | exclude**] {*source-address* | **source-list** [*acl*]}
	Example:
	`Router(config-if)# ipv6 mld static-group`
	`ff04::10 include 100::1`
		Configures forwarding of traffic for the multicast group onto this interface and behave as if an MLD joiner was present on the interface. The packets to the group get fastswitched or hardware switched (whatever is available on the platform).
		Note This command is not a sufficient condition for traffic to be forwarded onto the interface. Other conditions such as absence of a route, not being the DR or losing an assert can cause the router to not forward traffic even if the command is configured.

Configuring MLD Snooping

MLD snooping is not enabled by default. You have to configure it globally, which enables snooping on all the VLANs.

You can enable and disable MLD snooping on a per-VLAN basis. However, if you disable MLD snooping globally, it is disabled on all the VLANs. If global snooping is enabled, you can enable or disable VLAN snooping.

Restrictions

Cisco ASR 901 Routers support only the following encapsulations for MLD snooping:

- Untagged
- Dot1q (with or without rewrite)
- Routed QinQ (with rewrite pop 2)

The following commands are not supported: **ipv6 mld snooping tcn flood** and **ipv6 mld snooping tcn query solicit**.

Note In the context of REP and G8032, topology change may cause the routers in the ring topology to trigger general queries that may impact the convergence time (because this time is based on the report received from the host).

Enabling MLD Snooping Globally

To enable MLD snooping globally on the router, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping** **Example:** `Router(config)# ipv6 mld snooping`	Enables MLD snooping globally.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Enabling MLD Snooping on a VLAN

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

Procedure

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

	Command or Action	Purpose
Step 3	**ipv6 mld snooping** **Example:** `Router(config)# ipv6 mld snooping`	Enables MLD snooping globally.
Step 4	**ipv6 mld snoopingvlan** *vlan-id* **Example:** `Router(config)# ipv6 mld snooping vlan 1001`	Enables MLD snooping on the VLAN. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.

Step 5	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Configuring a Static Multicast Group

Hosts or Layer 2 ports normally join multicast groups dynamically. However, you can also statically configure an IPv6 multicast address and member ports for a VLAN.

To add a Layer 2 port as a member of a multicast group, perform this task:

Procedure

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

Step 3	**ipv6 mld snoopingvlan** *vlan-id* **static** *ipv6-multicast-address* **interface** *interface-id*
	Example:
	`Router(config)# ipv6 mld snooping vlan 104`
	`static FF45::5 interface gigabitethernet0/4`
		Configures statically a multicast group with a Layer 2 port as a member of a multicast group:
		• *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
		• *ipv6-multicast-address*— The 128-bit group IPv6 address. The address must be in the form specified in RFC 2373.
		• *interface-id*—The member port. It can be a physical interface or a port channel.

Step 4	**end** **Example:**	Exits global configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
	`Router(config)# end`	

Configuring a Multicast Router Port

To add a multicast router port to a VLAN, perform this task:

Procedure

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

Step 3	**ipv6 mld snoopingvlan** *vlan-id* **mroute interface** *interface-id*
	Example:
	`Router(config)# ipv6 mld snooping vlan 104`
	`mrouter interface gigabitEthernet 0/4`
		Specifies the multicast router VLAN ID, and the interface of the multicast router.
		• *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
		• *interface-id*—The member port. It can be a physical interface or a port channel.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Enabling MLD Immediate Leave

To enable MLDv1 Immediate Leave, follow these steps:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**ipv6 mld snoopingvlan** *vlan-id* **immediate-leave** **Example:** `Router(config)# ipv6 mld snooping vlan 104 immediate-leave`	Enables MLD Immediate Leave on the VLAN interface.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Configuring an MLD Snooping Query

To configure MLD snooping query characteristics for the router or for a VLAN, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping check hop-count** **Example:** `Router(config)# ipv6 mld snooping check hop-count`	Enables hop-count checking.
Step 4	**ipv6 mld snooping explicit-tracking limit** *limit* **Example:** `Router(config)# ipv6 mld snooping explicit-tracking limit 1000`	Enables explicit host tracking.
Step 5	**ipv6 mld snooping last-listener-query-count** *count* **Example:** `Router(config)# ipv6 mld snooping last-listener-query-count 3`	Sets the last listener query count on a VLAN basis. This value overrides the value configured globally. The range is from 1 to 7. The default is 0. When set to 0, the global count value is used. Queries are sent 1 second apart.

	Command or Action	Purpose
Step 6	**ipv6 mld snooping last-listener-query-interval** *interval* **Example:** `Router(config)# ipv6 mld snooping last-listener-query-interval 1000`	Sets the maximum response time that the switch waits for after sending out a MASQ before deleting a port from the multicast group. The range is from 100 to 32,768 thousandth of a second. The default is 1000 (1 second).
Step 7	**ipv6 mld snooping listener-message-suppression** **Example:** `Router(config)# ipv6 mld snooping listener-message-suppression`	Enables listener message suppression.
Step 8	**ipv6 mld snooping robustness-variable** *interval* **Example:** `Router(config)# ipv6 mld snooping robustness-variable 3`	Sets the number of queries that are sent before the router deletes a listener (port) that does not respond to a general query. The range is from 1 to 3. The default is 2.
Step 9	**ipv6 mld snooping vlan** *vlan-id* **Example:** `Router(config)# ipv6 mld snooping vlan 104`	Enables MLD snooping for VLAN. • *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.

Step 10	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Disabling MLD Listener Message Suppression

To disable MLD listener message suppression, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ipv6 mld snooping listener-message-suppression**	Disables listener message suppression.

	Command or Action	Purpose
	Example: `Router(config)# no ipv6 mld snooping listener-message-suppression`	

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Configuring a Rendezvous Point

To configure a rendezvous point (RP) in a Protocol Independent Multicast sparse mode (PIM-SM) network, see the Configuring a Rendezvous Point guide at:

http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

This guide provides scenario descriptions and basic configuration examples for the following options:

- Static RP
- Bootstrap router
- Anycast RP

Configuring PIM SSM Options

To configure PIM Source-Specific Multicast options, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 104`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 pim** **Example:** `Router(config-if)# ipv6 pim`	Configures PIM, if it is disabled. PIM runs on every interface after configuring IPv6 multicast routing.

	Command or Action	Purpose
Step 5	**ipv6 pim hello-interval** *interval-in-seconds* **Example:** `Router(config-if)# ipv6 pim hello-interval 45`	Configures periodic hello interval for this interface. Default is 30 seconds. Periodic hellos are sent out at intervals randomized by a small amount instead of on exact periodic interval.
Step 6	**ipv6 pim join-prune-interval** *interval-in-seconds* **Example:** `Router(config-if)# ipv6 pim join-prune-interval 75`	Configures periodic Join-Prune announcement interval for this interface. Default is 60 seconds.

Disabling PIM SSM Multicast on an Interface

To disable PIM SSM multicast on a specified interface, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 104`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**no ipv6 pim** **Example:** `Router(config-if)# no ipv6 pim`	Disables PIM on the specified interface.

Configuring IPv6 SSM Mapping

When the SSM mapping feature is enabled, DNS-based SSM mapping is automatically enabled, which means that the device looks up the source of a multicast MLD version 1 report from a DNS server.

You can configure either DNS-based or static SSM mapping, depending on your device configuration. If you choose to use static SSM mapping, you can configure multiple static SSM mappings. If multiple static SSM mappings are configured, the source addresses of all matching access lists are used.

To configure IPv6 SSM mapping, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable** **Example:** `Router(config-if)# ipv6 mld ssm-map enable`	Enables the SSM mapping feature for groups in the configured SSM range. **Note** You should first create ACL to define the group that needs to be mapped.
Step 4	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address* **Example:** `Router(config-if)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	Configures static SSM mappings.
Step 5	**no ipv6 mld** [**vrf** *vrf-name*] **ssm-map query dns** **Example:** `Router(config-if)# no ipv6 mld ssm-map query dns`	Disables DNS-based SSM mapping. **Note** You must disable SSM-map query dns when static mapping is configured.

Configuring IPv6 Multicast Routing for VRF Lite

To configure IPv6 multicast routing for VRF Lite, perform this task:

Procedure

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast-routing vrf** *vrf-name* **Example:** `Router(config)# ipv6 multicast-routing vrf vpe_1`	Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router.
Step 4	**vrf definition***vrf-name* **Example:** `Router(config-vrf)# vrf definition vpe_1`	Configures a VRF routing table instance and enter VRF configuration mode.
Step 5	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 1.1.1.1:100`	Specifies a route distinguisher (RD) for a VRF instance. The *route-distinguisher* is an 8-byte value to be added to an IPv6 prefix to create a VPN IPv6 prefix.
Step 6	**address-family ipv6** **Example:** `Router(config-vrf)# address-family ipv6`	Specifies the address family submode for configuring routing protocols.
Step 7	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits the address family submode.

Enabling VRF Under a VLAN Interface

To configure VRF under a VLAN interface, perform this task:

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Router(config-if)# vrf forwarding vpe_1`	Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface or subinterface. The *vrf-name* is the name assigned to a VRF.
Step 5	**ipv6 address** *ipv6-address* **Example:** `Router(config-if)# ipv6 address my-prefix 0:0:0:7272::72/64`	Configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.

Configuring PIM BFD on an IPv6 Interface

To configure PIM BFD on an IPv6 interface, perform this task:

Restriction

- This feature is supported only on switch virtual interfaces on which both PIM and BFD are supported.
- For ECMP, PIM BFD is used to detect quick neighbor failure.
- For non-ECMP, BFD for IGP should be configured for faster convergence.
- Timers that are less than 50 ms for 3 sessions are not supported.

Before you begin

- IPv6 multicast must be enabled and Protocol Independent Multicast (PIM) must be configured on the interface.
- Ensure that Bidirectional Forwarding Detection (BFD) for IGP is always configured along with PIM.

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 pim bfd** **Example:** `Router(config-if)# ipv6 pim bfd`	Enables PIMv6 BFD on an interface.

Verifying IPv6 Multicast

Use the **show** commands listed below to verify the IPv6 Multicast configuration.

To display the group membership information on various interfaces on a router, use the **show** command described in the following example.

```
Router# show ipv6 mld groups

MLD Connected Group Membership
Group Address                           Interface          Uptime    Expires
FF04::10                                Vlan104            00:18:41  never
FF04::12                                Vlan104            00:19:10  never
FF34::4                                 Vlan104            00:35:00  not used
FF45::5                                 Vlan104            00:35:04  00:01:44
```

To display the MLD interface specific parameters, use the **show** command described in the following example.

```
Router# show ipv6 mld interface vlan 104

Vlan104 is up, line protocol is up
Internet address is FE80::4255:39FF:FE89:6283/10
MLD is enabled on interface
Current MLD version is 2
MLD query interval is 60 seconds
MLD querier timeout is 130 seconds
MLD max query response time is 20 seconds
Last member query response interval is 1 seconds
MLD activity: 18 joins, 7 leaves
MLD querying router is FE80::4255:39FF:FE89:6283 (this system)
```

To display the MLD traffic counters, use the **show** command described in the following example.

```
Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared: 02:29:12

                              Received     Sent
Valid MLD Packets               784         385
Queries                         4           167
Reports                         776         218
Leaves                          4           0
Mtrace packets                  0           0
```

```
Errors:
Malformed Packets                           0
Martian source                              10
Non link-local source                       0
Hop limit is not equal to 1                 0
```

To display interface specific information for PIM, use the **show** command described in the following example.

```
Router# show ipv6 pim interface

Interface          PIM   Nbr   Hello  DR
                         Count Intvl  Prior

Vlan102            on    1     30     1
    Address: FE80::4255:39FF:FE89:5283
    DR     : FE80::4255:39FF:FE89:5284
Null0              off    0     30     1
    Address: FE80::1
    DR     : not elected
FastEthernet0/0    off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/8 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/9 off    0     30     1
    Address: ::
    DR     : not elected
Gi0/10             off    0     30     1
    Address: ::
    DR     : not elected
Gi0/11             off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/0 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/1 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/2 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/3 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/4 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/5 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/6 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/7 off    0     30     1
    Address: ::
    DR     : not elected
Vlan1              off    0     30     1
    Address: ::
    DR     : not elected
Port-channel1      off    0     30     1
    Address: ::
```

```
    DR      : not elected
Tunnel0            off    0     30     1
    Address: FE80::7EAD:74FF:FE9D:94C8
    DR      : not elected
Loopback1          off    0     30     1
    Address: ::
    DR      : not elected
Vlan104            on    1     45     1
    Address: FE80::4255:39FF:FE89:6283
    DR      : FE80::4255:39FF:FE89:6284
Tunnel1            off    0     30     1
    Address: FE80::7EAD:74FF:FE9D:94C8
    DR      : not elected
```

To display the number of (*, G) and (S, G) membership reports present in the MLD cache, use the **show** command described in the following example.

```
Router# show ipv6 mld groups summary

MLD Route Summary
  No. of (*,G) routes = 9
  No. of (S,G) routes = 3
```

To display the number of PIM neighbors on each interface, as well as, the total number of PIM neighbors, use the **show** command described in the following example.

```
Router# show ipv6 pim neighbor count

Interface          Nbr count

Vlan104            1
Vlan102            1

Total Nbrs         2
```

To display the number of PIM neighbors discovered, use the **show** command described in the following example.

```
Router# show ipv6 pim neighbor

PIM Neighbor Table
Mode: B - Bidir Capable, G - GenID Capable
Neighbor Address           Interface          Uptime    Expires  Mode DR pri

FE80::4255:39FF:FE89:5284  Vlan102            02:30:51  00:01:38 B G  DR 1
FE80::4255:39FF:FE89:6284  Vlan104            00:09:49  00:01:16 B G  DR 1
```

To display the information in the PIM topology table in a format similar to the **show ip mroute** command, use the show command described in the following example.

```
Router# show ipv6 mroute

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

(2006::1, FF34::4), 00:38:41/never, flags: sPTI
  Incoming interface: Vlan102
  RPF nbr: FE80::4255:39FF:FE89:5284
  Immediate Outgoing interface list:
    Vlan104, Null, 00:38:41/never

(100::1, FF04::10), 00:22:21/never, flags: SPI
  Incoming interface: Null
  RPF nbr: ::
  Immediate Outgoing interface list:
    Vlan104, Null, 00:22:21/never

(*, FF04::12), 00:22:50/never, RP 2021::2021, flags: SPCL
  Incoming interface: Vlan104
  RPF nbr: FE80::4255:39FF:FE89:6284
  Outgoing interface list: Null

(2001:DB8::10:11, FF04::12), 00:22:50/never, RP 2021::2021, flags: SPLRI
  Incoming interface: Vlan104
  RPF nbr: FE80::4255:39FF:FE89:6284
  Outgoing interface list: Null

(*, FF45::5), 00:38:44/never, RP 2021::2021, flags: SPC
  Incoming interface: Vlan104
  RPF nbr: FE80::4255:39FF:FE89:6284
  Outgoing interface list: Null
```

To display PIM topology table for given group or all groups, use the **show** command described in the following example.

```
Router# show ipv6 pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info Upstream Mode
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected, Y - Joined MDT-data group,
    y - Sending to MDT-data group
    BGS - BGP Signal Sent, !BGS - BGP signal suppressed
    SAS - BGP Src-Act Sent, SAR - BGP Src-Act Received
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, BS - BGP Signal,
    BP - BGP Shared-Tree Prune, BPT - BGP Prune Time

(2006::1,FF34::4)
SSM SPT UP: 00:39:23 JP: Null(never) Flags:
RPF: Vlan102,FE80::4255:39FF:FE89:5284
  Vlan104            00:39:23  off     LI

(100::1,FF04::10)
SM UP: 00:23:04 JP: Null(never) Flags:
```

```
RPF: ,::
  Vlan104            00:23:04  off     LI

(*,FF04::12)
SM UP: 00:23:33 JP: Null(never) Flags:
RP: 2021::2021
RPF: Vlan104,FE80::4255:39FF:FE89:6284
  Vlan104            00:23:33  off     LI II

(2001:DB8::10:11,FF04::12)
SM RPT UP: 00:23:33 JP: Null(never) Flags:
RP: 2021::2021
RPF: Vlan104,FE80::4255:39FF:FE89:6284
  Vlan104            00:23:33  off     LD ID

(*,FF45::5)
SM UP: 00:39:27 JP: Null(never) Flags:
RP: 2021::2021
RPF: Vlan104,FE80::4255:39FF:FE89:6284
  Vlan104            00:39:27  off     LI IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
RR - Register Received, SR - Sending Registers,
E - MSDP External, DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF0E::E0:1:1:1)
SM UP: 04:27:50 JP: Join(never) Flags: LH
RP: 51::1:1:2*
RPF: Tunnel1,51::1:1:2*
FastEthernet4/10 04:27:50 fwd Join(00:02:48) LI LH
(47::1:1:3,FF0E::E0:1:1:1)
SM SPT UP: 04:27:20 JP: Join(never) Flags: KAT(00:01:04) AA PA RA SR
RPF: Vlan47,47::1:1:3*
FastEthernet4/10 04:27:16 fwd Join(00:03:14)
Tunnel0 04:27:17 fwd
```

To display the count of the ranges, (*, G), (S, G) and (S, G) RPT routes in the pim topology tables, use the **show** command described in the following example.

```
Router# show ipv6 pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 47
  No. of (*,G) routes = 11
  No. of (S,G) routes = 2
  No. of (S,G)RPT routes = 1
```

To display the IP multicast group mapping table, use the **show** command described in the following example. It shows group to mode mapping and RP information in case of sparse-mode groups.

```
Router# show ipv6 pim group-map FF0E::E0:1:1:1

IP PIM Group Mapping Table
(* indicates group mappings being used)

FF00::/8*
    SM, RP: 2021::2021
    RPF: Vl104,FE80::4255:39FF:FE89:6284
    Info source: Static
    Uptime: 02:33:31, Groups: 3
```

To display the IPv6 multicast range-lists on a per client (config/autorp/BSR) and per mode (SSM/SM/DM/Bidir) basis, use the **show** command described in the following example.

```
Router# show ipv6 pim range-list

Static SSM Exp: never Learnt from : ::
  FF33::/32 Up: 02:33:46
  FF34::/32 Up: 02:33:46
  FF35::/32 Up: 02:33:46
  FF36::/32 Up: 02:33:46
  FF37::/32 Up: 02:33:46
  FF38::/32 Up: 02:33:46
  FF39::/32 Up: 02:33:46
  FF3A::/32 Up: 02:33:46
  FF3B::/32 Up: 02:33:46
  FF3C::/32 Up: 02:33:46
  FF3D::/32 Up: 02:33:46
  FF3E::/32 Up: 02:33:46
  FF3F::/32 Up: 02:33:46
Static SM RP: 2021::2021 Exp: never Learnt from : ::
  FF00::/8 Up: 02:33:44
```

To display information about the PIM register encapsulation and decapsulation tunnels, use the **show** command described in the following example.

```
Router# show ipv6 pim tunnel

Tunnel0*
  Type  : PIM Encap
  RP    : Embedded RP Tunnel
  Source: 2003::2
Tunnel1*
  Type  : PIM Encap
  RP    : 2021::2021
  Source: 2003::2
```

To display information about the PIM traffic counters, use the **show** command described in the following example.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 02:34:35

                              Received     Sent
Valid PIM Packets               613         629
Hello                           613         622
Join-Prune                      0           7
Data Register                   0           -
Null Register                   0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
```

```
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets drops due to PIM queue limits       0
```

To display the average Join/Prune aggregation for the last (1000/10000/50000) packets for each interface, use the **show** command described in the following example.

```
Router# show ipv6 pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          MTU        Transmitted            Received

Vlan102            1500       0    / 0    / 0         0    / 0    / 0
Null0              1500       0    / 0    / 0         0    / 0    / 0
FastEthernet0/0    1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/8 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/9 1280       0    / 0    / 0         0    / 0    / 0
Gi0/10             1280       0    / 0    / 0         0    / 0    / 0
Gi0/11             1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/0 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/1 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/2 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/3 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/4 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/5 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/6 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/7 1280       0    / 0    / 0         0    / 0    / 0
Vlan1              1280       0    / 0    / 0         0    / 0    / 0
Port-channel1      1280       0    / 0    / 0         0    / 0    / 0
Tunnel0            1452       0    / 0    / 0         0    / 0    / 0
Loopback1          1280       0    / 0    / 0         0    / 0    / 0
Vlan104            1500       0    / 0    / 0         0    / 0    / 0
Tunnel1            1452       0    / 0    / 0         0    / 0    / 0
```

To display the MRIB table, use the **show** command described in the following example. All entries are created by various clients of MRIB, such as, MLD, PIM and MFIB. The flags on each entry or interface, serve as communication mechanism between various clients of MRIB.

```
Router# show ipv6 mrib route FF0E::E0:1:1:1

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
    ET - Data Rate Exceeds Threshold,K - Keepalive,DDE - Data Driven Event
    ME - MoFRR ECMP Flow based, MNE - MoFRR Non-ECMP Flow based,
    MP - Primary MoFRR Non-ECMP Flow based entry
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, MD - mCAC Denied, MI - mLDP Interest
    A2 - MoFRR ECMP Backup Accept

(*,FF45::5) RPF nbr: FE80::4255:39FF:FE89:6284 Flags: C
  Vlan104 Flags: A LI
```

To display the count of the number of routes in the Multicast RIB, use the **show** command described in the following example.

```
Router# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 57
  No. of (S,G) routes = 3
  No. of Route x Interfaces (RxI) = 22
```

To display information about the various MRIB clients, use the **show** command described in the following example.

```
Router# show ipv6 mrib client

IP MRIB client-connections
igmp (0x0):309  (connection id 1)
pim (0x0):342   (connection id 2)
IPv6_mfib(0x1031AFB0):0.358     (connection id 3)

2024#show ipv6 mfib ff45::5
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
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
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, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

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
 (*,FF45::5) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Vlan104 Flags: A
```

To display information about the IPv6 Multicast Forwarding Information Base, in terms of forwarding entries and interfaces, use the **show** command described in the following example.

```
Router# show ipv6 mfib FF0E::E0:1:1:1

IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF0E::E0:1:1:1) Flags: C
Forwarding: 0/0/0/0, Other: 0/0/0
Tunnel1 Flags: A NS
FastEthernet4/10 Flags: F NS
```

```
Pkts: 0/0
(47::1:1:3,FF0E::E0:1:1:1) Flags:
Forwarding: 9592618/0/182/0, Other: 0/0/0
Vlan47 Flags: A
Tunnel0 Flags: F NS
Pkts: 0/0
FastEthernet4/10 Flags: F NS
Pkts: 0/9592618
```

To display the general MFIB configuration status and operational status, use the **show** command described in the following example.

```
Router# show ipv6 mfib status

IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 358
    Tables 1/1/0 (active/mrib/io)
```

To display summary information about the number of IPv6 MFIB entries and interfaces, use the **show** command described in the following example.

```
Router# show ipv6 mfib summary

Default
 60 prefixes (60/0/0 fwd/non-fwd/deleted)
 21 ioitems (21/0/0 fwd/non-fwd/deleted)
 Forwarding prefixes: [3 (S,G), 11 (*,G), 46 (*,G/m)]
 Table id 0x0, instance 0x1031AFB0
 Database: epoch 0

2024#show ipv6 mfib in
2024#show ipv6 mfib int
2024#show ipv6 mfib interface
IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 358
    Tables 1/1/0 (active/mrib/io)

MFIB interface             status    CEF-based output
                                  [configured,available]
Vlan102                    up     [yes       ,yes      ]
Vlan104                    up     [yes       ,yes      ]
Tunnel0                    up     [yes       ,no       ]
Tunnel1                    up     [yes       ,yes      ]
```

To display the IPv6 multicast-enabled interfaces and their forwarding status, use the **show** command described in the following example.

```
Router# show ipv6 mfib interface

IPv6 Multicast Forwarding (MFIB) status:
Configuration Status: enabled
```

```
Operational Status: running
MFIB interface status CEF-based output
[configured,available]
Loopback0 up [yes ,? ]
Vlan46 up [yes ,? ]
Vlan47 up [yes ,? ]
Tunnel0 down [yes ,no ]
Tunnel1 down [yes ,no ]
```

To display how IPv6 multicast routing does Reverse Path Forwarding, use the **show** command described in the following example.

```
Router# show ipv6 rpf FE80::4255:39FF:FE89:7404

RPF information for 3::3
  RPF interface: Vlan10
  RPF neighbor: FE80::4255:39FF:FE89:7404
  RPF route/mask: 3::3/128
  RPF type: Unicast
  RPF recursion count: 0
  Metric preference: 110
  Metric: 2
```

Verifying MLD Snooping

Use the **show** commands listed below to verify the MLD snooping configuration.

To verify whether IPv6 MLD snooping report suppression is enabled or disabled, use the **show** command used in the following example:

```
Router# show ipv6 mld snooping

Global MLD Snooping configuration:
-------------------------------------------
MLD snooping Oper State      : Enabled
MLDv2 snooping               : Enabled
Listener message suppression : Disabled
EHT DB limit/count           : 1000/2
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 3
Last listener query count    : 3
Last listener query interval : 1000
Check Hop-count=1            : Yes

Vlan 102:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Disabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/0
Check Hop-count=1                   : Yes

Vlan 104:
--------
```

```
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Enabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/2
Check Hop-count=1                   : Yes

Vlan 1001:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Disabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/0
Check Hop-count=1                   : Yes
```

To display all or a specified IP Version 6 (IPv6) multicast address information maintained by MLD snooping, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping address

Flags: M -- MLD snooping, S -- Static

Vlan Group/source Type Version Port List
-----------------------------------------------------------------------
104 FF34::1 M v2 Gi0/6 Gi0/10 Po1
/2006::1 M Gi0/6 Gi0/10 Po1
104 FF34::2 M v2 Gi0/6 Gi0/10 Po1
/2006::1 M Gi0/6 Gi0/10 Po1
104 FF34::3 M v2 Gi0/6 Gi0/10 Po1
/2006::1 M Gi0/6 Gi0/10 Po1
104 FF02::FB M v2 Gi0/0
```

To display the number of multicast groups on a router or in a specified VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping address count

Total number of groups: 4
Total number of (S,G): 3
```

To display the MLD snooping membership summary on a router or in a specified VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping membership

Snooping Membership Summary for Vlan 104
------------------------------------------
Total number of channels: 1
Total number of hosts   : 2

Source/Group                  Interface Reporter                      Uptime   Last-Join/
```

```
                                                                                 Last-Leave
-------------------------------------------------------------------------------------------

2006::1/FF34::4                 Gi0/1     FE80::4255:39FF:FE89:6284       00:47:22 00:00:11
 /
                                                                                        -


2006::1/FF34::4                 Gi0/10    FE80::200:4EFF:FE72:F91F        00:47:26 00:00:09
 /
                                                                                        -
```

To display the MLD snooping that is dynamically learned and manually configured on the multicast router ports for a router or for a specific multicast VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping mrouter

Vlan    ports
----    -----
 102    Po1(dynamic)
 104    Gi0/1(dynamic), Gi0/4(static)
```

To display the configuration and operation information for the MLD snooping configured on a router, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping querier

Vlan      IP Address               MLD Version   Port
-------------------------------------------------------------
102       FE80::4255:39FF:FE89:5284
                                   v2            Po1
104       FE80::4255:39FF:FE89:6284
                                   v2            Gi0/1
```

To verify a static member port and an IPv6 address, use the **show** command described in the following example:

```
Router# show mac-address-table multicast mld-snooping

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
```

To verify if IPv6 MLD snooping is enabled on a VLAN interface, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping mrouter vlan 104

Vlan    ports
----    -----
 104    Gi0/1(dynamic), Gi0/4(static)
```

To verify if Immediate Leave is enabled on a VLAN interface, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping vlan 104

Global MLD Snooping configuration:
-------------------------------------------
MLD snooping Oper State      : Enabled
MLDv2 snooping               : Enabled
```

```
Listener message suppression : Disabled
EHT DB limit/count           : 1000/2
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 3
Last listener query count    : 3
Last listener query interval : 1000
Check Hop-count=1            : Yes

Vlan 104:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Enabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/2
Check Hop-count=1                   : Yes
Query Interval                      : 125
Max Response Time                   : 10000
```

To verify the MLD snooping querier information for a router or for a VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping querier vlan 102

IP address               : FE80::4255:39FF:FE89:5284
MLD  version             : v2
Port                     : Gi0/3
Max response time        : 10s
Query interval           : 125s
Robustness variable      : 2
```

Verifying IPv6 Multicast Routing for VRF Lite

Use the **show** commands listed below to verify IPv6 multicast routing for VRF Lite configuration.

To view information about the interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command:

```
Router# show ipv6 pim vrf VPN_B interface

Interface          PIM   Nbr   Hello  DR
                         Count Intvl  Prior

Vlan122            on     1     30     1
    Address: FE80::7EAD:74FF:FEDC:E4AC
    DR     : this system
Vlan123            on     1     30     1
    Address: FE80::7EAD:74FF:FEDC:E4AC
    DR     : this system
Tunnel1            off     0     30     1
    Address: FE80::7EAD:74FF:FEDC:E4B0
    DR     : not elected
```

To view the information in a PIM topology table, use the **show ipv6 mroute** command:

```
Router# show ipv6 mroute vrf VPN_B

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

(170:1::3, FF36::1), 21:11:23/00:03:23, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:23

(170:1::3, FF36::2), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::3), 21:11:23/00:02:33, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:02:33

(170:1::3, FF36::4), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::5), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::6), 21:11:23/00:02:33, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:02:33

(170:1::3, FF36::7), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::8), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::9), 21:11:23/00:03:13, flags: sT
```

```
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::A), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

Pura-5#
```

To view the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB), use the **show ipv6 mfib** command:

```
Router# show ipv6 mfib vrf VPN_B

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
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
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, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

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
VRF VPN_B
 (*,FF00::/8) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF00::/15) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF02::/16) Flags:
   SW Forwarding: 0/0/0/0, Other: 4/4/0
 (*,FF10::/15) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF12::/16) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF20::/15) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF22::/16) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF30::/15) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF32::/16) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF33::/32) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF34::/32) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF35::/32) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF36::/32) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (170:1::3,FF36::1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
```

```
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::2) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::3) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::4) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::5) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::6) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::7) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::8) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::9) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::A) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(*,FF37::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF38::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF39::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3A::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3B::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3C::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3D::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3E::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3F::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF40::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF42::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF50::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF52::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF60::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF62::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF70::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF72::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF80::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF82::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF90::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF92::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFA0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFA2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFB0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFB2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFC0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFC2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFD0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFD2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFE0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFE2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFF0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFF2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
```

Verifying PIM BFD Support

Use the **show** commands listed below to verify PIM BFD support.

To view a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **show bfd neighbors ipv6** command:

```
Router# show bfd neighbors ipv6

IPv6 Sessions
NeighAddr LD/RD RH/RS State Int
FE80::4255:39FF:FE89:5284 4/4 Up Up Vl24
FE80::FE99:47FF:FE37:FBC0 2/4 Up Up Vl101
```

To view all BFD protocol parameters, timers, and clients such as PIM, OSPF, and so on for each neighbor, use the **show bfd neighbors ipv6 details** command:

```
Router# show bfd neighbors ipv6 details

IPv6 Sessions
NeighAddr LD/RD RH/RS State Int
FE80::4255:39FF:FE89:5284 4/4 Up Up Vl24
Session state is UP and not using echo function.
Session Host: Software
OurAddr: FE80::4255:39FF:FE89:6284
Handle: 4
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 110(0), Hello (hits): 50(52910)
Rx Count: 52927, Rx Interval (ms) min/max/avg: 1/56/45 last: 40 ms ago
Tx Count: 52912, Tx Interval (ms) min/max/avg: 1/56/45 last: 12 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPFv3
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 5 last_rx_auth_seq 4
Uptime: 00:40:05
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 4 - Your Discr.: 4
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0

IPv6 Sessions
NeighAddr LD/RD RH/RS State Int
FE80::FE99:47FF:FE37:FBC0 2/4 Up Up Vl101
Session state is UP and not using echo function.
Session Host: Software
OurAddr: FE80::4255:39FF:FE89:6284
Handle: 2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 142(0), Hello (hits): 50(53327)
Rx Count: 53317, Rx Interval (ms) min/max/avg: 1/56/45 last: 8 ms ago
Tx Count: 53330, Tx Interval (ms) min/max/avg: 1/56/46 last: 24 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPFv3
```

```
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 4 last_rx_auth_seq 5
Uptime: 00:40:24
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 4 - Your Discr.: 2
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0
```

Configuration Examples for IPv6 Multicast

Example: Enabling IPv6 Multicast Routing

The following is a sample configuration of IPv6 Multicast feature on the Cisco ASR 901 Router.

```
!
!
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
asr901-platf-multicast enable
!
!
```

Example: Configuring IPv6 SSM Mapping

The following is a sample configuration of IPv6 SSM mapping on the Cisco ASR 901 router.

```
!
!
ipv6 mld ssm-map enable
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1
ipv6 mld ssm-map query dns
!
!
```

Example: Configuring IPv6 MLD Snooping

The following is a sample configuration of IPv6 MLD snooping on a Cisco ASR 901 Router.

```
!
Building configuration...
!
!
!
!
asr901-platf-multicast enable
ip multicast-routing
ipv6 unicast-routing
```

```
ipv6 cef
ipv6 mld snooping explicit-tracking limit 1000
ipv6 mld snooping check hop-count
ipv6 mld snooping robustness-variable 3
ipv6 mld snooping last-listener-query-count 6
ipv6 mld snooping last-listener-query-interval 10000
ipv6 mld snooping vlan 104 mrouter interface Gi0/4
ipv6 mld snooping vlan 104 immediate-leave
ipv6 mld snooping vlan 104 static FF45::5 interface Gi0/4
ipv6 mld snooping
ipv6 multicast-routing
!
!
```

Example: Configuring Rendezvous Point

For a sample configuration of RP, see the *Configuring a Rendezvous Point* document at: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Example: Configuring IPv6 Multicast Routing for VRF Lite

The following is a sample configuration of IPv6 multicast routing for VRF Lite:

```
Building configuration...

!
!
!
vrf definition vpe_2
 rd 1.1.1.1:100
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
!
!
ipv6 multicast-routing
ipv6 multicast-routing vrf VPN_B
ipv6 multicast-routing vrf VPN_C
ipv6 multicast-routing vrf vpe_2
!
!
!
multilink bundle-name authenticated
l3-over-l2 flush buffers
asr901-platf-multicast enable
asr901-storm-control-bpdu 1000
!
!
!
interface Vlan80
 vrf forwarding vpe_2
 ip address 192.108.1.27 255.255.255.0
 ip pim sparse-mode
 ipv6 address my-prefix ::7272:0:0:0:72/64
```

```
!
!
!
end
```

Example: Configuring BFD PIM on an IPv6 Interface

The following is a sample configuration of BFD PIM on an IPv6 interface:

```
!
Building configuration...

Current configuration : 6679 bytes
!
! Last configuration change at 17:03:42 IST Wed May 21 2014
!

hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone IST 5 30
ip cef
!
!
!
!
no ip domain lookup

ip multicast-routing
ipv6 unicast-routing
ipv6 cef
ipv6 mld snooping
ipv6 multicast-routing
!
!

asr901-platf-multicast enable

!
interface Loopback1
ip address 3.3.3.3 255.255.255.255

interface GigabitEthernet0/0

service instance 24 ethernet
encapsulation dot1q 24
rewrite ingress tag pop 1 symmetric
bridge-domain 24

!
interface Vlan24
ipv6 address 2024::2/64
ipv6 pim bfd
ipv6 ospf 1 area 0
bfd interval 50 min_rx 50 multiplier 3
```

```
ipv6 router ospf 1
router-id 3.3.3.3
bfd all-interfaces
timers throttle spf 50 50 5000
timers throttle lsa 10 20 5000
timers lsa arrival 10
timers pacing flood 5
!
!

!
!
end
```

Troubleshooting Tips

Use the following **debug** commands to enable the debug feature to help troubleshoot the IPv6 Multicast feature on the Cisco ASR 901 Router.

Note We recommend that you do not use these **debug** commands without TAC supervision.

Command Name	Description
[no] debug ipv6 mld	Enables debugging MLD protocol activity.
[no] debug ipv6 mld snooping	Enables debugging IPv6 MLD snooping activity.
[no] debug ipv6 pim	Enables debugging PIM protocol activity.
[no] debug ipv6 pim neighbor	Enables debugging for PIM Hello message processing.
[no] debug ipv6 mrib route	Enables debugging MRIB routing entry related activity.
[no] debug ipv6 mrib client	Enables debugging MRIB client management activity.
[no] debug ipv6 mrib io	Enables debugging MRIB I/O events.
[no] debug ipv6 mrib table	Enables debugging MRIB table management activity.
[no] debug platform hardware cef ip multicast	
[no] debug ip pim vrf	Enables debugging for PIM-related events.
[no] debug ipv6 pim neighbor	Enables debugging on PIM protocol activity.
[no] debug ipv6 pim bfd	Enables debugging on PIM protocol activity for BFD.
[no] debug bfd event	Enables debugging messages about BFD. on PIM protocol activity.