



# Implementing IPv6 Multicast

---

**Last Updated: April 18, 2012**

Traditional IP communication allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). IPv6 multicast provides a third scheme, allowing a host to send a single data stream to a subset of all hosts (group transmission) simultaneously.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Implementing IPv6 Multicast, page 1](#)
- [Restrictions for Implementing IPv6 Multicast, page 2](#)
- [Information About Implementing IPv6 Multicast, page 3](#)
- [How to Implement IPv6 Multicast, page 18](#)
- [Configuration Examples for Implementing IPv6 Multicast, page 75](#)
- [Additional References, page 80](#)
- [Feature Information for Implementing IPv6 Multicast, page 81](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites for Implementing IPv6 Multicast

- In order to enable IPv6 multicast routing on a router, you must first enable IPv6 unicast routing on the router. For information on how to enable IPv6 unicast routing on a router, refer to *Implementing IPv6 Addressing and Basic Connectivity*.
- You must enable IPv6 unicast routing on all interfaces.
- This module assumes that you are familiar with IPv6 addressing and basic configuration. Refer to the *Implementing IPv6 Addressing and Basic Connectivity* module for more information.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

## Restrictions for Implementing IPv6 Multicast

- IPv6 multicast for Cisco IOS software uses MLD version 2. This version of MLD is fully backward-compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 will interoperate with a router running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- IPv6 multicast is supported only over IPv4 tunnels in Cisco IOS Release 12.3(2)T, Cisco IOS Release 12.2(18)S, and Cisco IOS Release 12.0(26)S.
- When the bidirectional (bidir) range is used in a network, all routers in that network must be able to understand the bidirectional range in the bootstrap message (BSM).
- IPv6 multicast routing is disabled by default when the **ipv6 unicast-routing** command is configured. On Cisco Catalyst 6500 and Cisco 7600 series routers, the **ipv6 multicast-routing** also must be enabled in order to use IPv6 unicast routing.

### Platform-Specific Information and Restrictions

In Cisco IOS Release 12.0(26)S, IPv6 multicast is supported on the Cisco 12000 series Internet router only on the following line cards:

- IP Service Engine (ISE):
  - 4-port Gigabit Ethernet ISE
  - 4-port OC-3c/STM-1c POS/SDH ISE
  - 8-port OC-3c/STM-1c POS/SDH ISE
  - 16-port OC-3c/STM-1c POS/SDH ISE
  - 4-port OC-12c/STM-4c POS/SDH ISE
  - 1-port OC-48c/STM-16c POS/SDH ISE
- Engine 4 Plus (E4+) Packet-over-SONET (POS):
  - 4-port OC-48c/STM-16c POS/SDH
  - 1-port OC-192c/STM-64c POS/SDH

On Cisco 12000 series line cards, the IPv6 multicast feature includes support for Protocol Independent Multicast sparse mode (PIM-SM), Multicast Listener Discovery (MLDv2), static mroutes, and the IPv6 distributed Multicast Forwarding Information Base (MFIB).

Forwarding of IPv6 multicast traffic is hardware-based on Cisco 12000 series IP Service Engine (ISE) line cards that support IPv6 multicast and software-based on all other supported Cisco 12000 series line cards.

On Cisco 12000 series ISE line cards, IPv6 multicast is implemented so that if the number of IPv6 multicast routes exceeds the hardware capacity of the ternary content addressable memory (TCAM), the following error message is displayed to describe how to increase the TCAM hardware capacity for IPv6 multicast routes:

```
EE48-3-IPV6_TCAM_CAPACITY_EXCEEDED: IPv6 multicast pkts will be software switched.
To support more IPv6 multicast routes in hardware:
Get current TCAM usage with: show controllers ISE <slot> tcam
In config mode, reallocate TCAM regions e.g. reallocate Netflow TCAM to IPv6 Mcast
hw-module slot <num> tcam carve rx_ipv6_mcast <v6-mcast-percent>
hw-module slot <num> tcam carve rx_top_nf <nf-percent>
Verify with show command that sum of all TCAM regions = 100%
Reload the linecard for the new TCAM carve config to take effect
WARNING: Recarve may affect other input features(ACL,CAR,MQC,Netflow)
```

TCAM is used for IPv6 multicast forwarding lookups. To increase TCAM capacity for handling IPv6 multicast routes, you must use the **hw-module slot number tcam carve rx\_ipv6\_mcast v6-mcast-**

*percentage* command in privileged EXEC mode, where *v6-mcast-percentage* specifies the percentage of TCAM hardware used by IPv6 multicast prefix.

For example, you can change the IPv6 multicast region from 1 percent (default) to 16 percent of the TCAM hardware by reallocating the NetFlow region from 35 percent (default) to 20 percent as follows:

```
Router# hw-module slot 3 tcam carve rx_ipv6_mcast 16
Router# hw-module slot 3 tcam carve rx_nf 20
```

On Cisco 12000 series router with IPv6 multicast enabled, if you delete a subinterface with IPv6 configured or if IPv6 is disabled on a subinterface, the associated main interface gets reset.

**Note**

From Cisco IOS Release 12.0(32)SY11 and 12.0(33)S7, deleting a subinterface or disabling IPv6 on a subinterface will reset the associated main interface only if that subinterface is the last subinterface with IPv6 configured under the main interface.

IPv6 multicast hardware forwarding is supported on the Cisco Catalyst 6500 and 7600 series in Cisco IOS Release 12.2(18)SXE.

## Information About Implementing IPv6 Multicast

- [IPv6 Multicast Overview](#), page 3
- [IPv6 Multicast Addressing](#), page 4
- [IPv6 Multicast Routing Implementation](#), page 6
- [Multicast Listener Discovery Protocol for IPv6](#), page 7
- [Protocol Independent Multicast](#), page 9
- [Static Mroutes](#), page 16
- [MRIB](#), page 16
- [MFIB](#), page 16
- [IPv6 Multicast VRF Lite](#), page 17
- [IPv6 Multicast Process Switching and Fast Switching](#), page 17
- [Multiprotocol BGP for the IPv6 Multicast Address Family](#), page 18
- [NSF and SSO Support In IPv6 Multicast](#), page 18
- [Bandwidth-Based CAC for IPv6 Multicast](#), page 18

## 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 router. This signaling is achieved with the MLD protocol.

Routers 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.

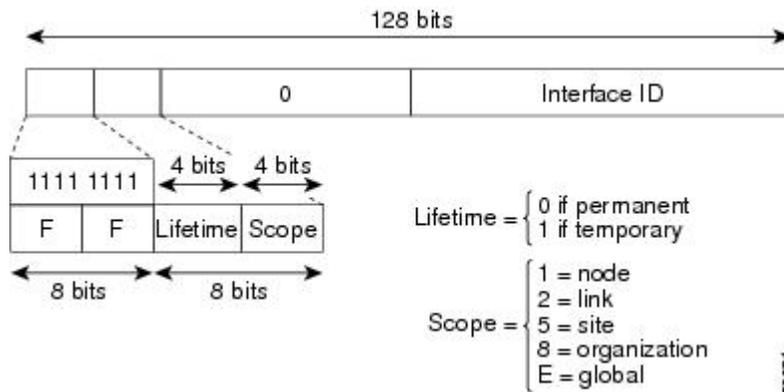
Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

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 Addressing

An IPv6 multicast address is an IPv6 address that has a prefix of FF00::/8 (1111 1111). An IPv6 multicast address is an identifier for a set of interfaces that typically belong to different nodes. A packet sent to a multicast address is delivered to all interfaces identified by the multicast address. The second octet following the prefix defines the lifetime and scope of the multicast address. A permanent multicast address has a lifetime parameter equal to 0; a temporary multicast address has a lifetime parameter equal to 1. A multicast address that has the scope of a node, link, site, or organization, or a global scope has a scope parameter of 1, 2, 5, 8, or E, respectively. For example, a multicast address with the prefix FF02::/16 is a permanent multicast address with a link scope. The figure below shows the format of the IPv6 multicast address.

**Figure 1** IPv6 Multicast Address Format



IPv6 nodes (hosts and routers) are required to join (receive packets destined for) the following multicast groups:

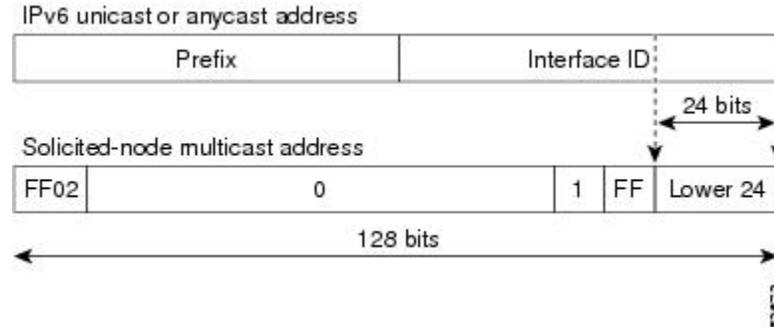
- All-nodes multicast group FF02:0:0:0:0:0:1 (scope is link-local)
- Solicited-node multicast group FF02:0:0:0:1:FF00:0000/104 for each of its assigned unicast and anycast addresses

IPv6 routers must also join the all-routers multicast group FF02:0:0:0:0:0:2 (scope is link-local).

The solicited-node multicast address is a multicast group that corresponds to an IPv6 unicast or anycast address. IPv6 nodes must join the associated solicited-node multicast group for every unicast and anycast address to which it is assigned. The IPv6 solicited-node multicast address has the prefix FF02:0:0:0:1:FF00:0000/104 concatenated with the 24 low-order bits of a corresponding IPv6 unicast or anycast address (see the figure below). For example, the solicited-node multicast address corresponding to

the IPv6 address 2037::01:800:200E:8C6C is FF02::1:FF0E:8C6C. Solicited-node addresses are used in neighbor solicitation messages.

**Figure 2 IPv6 Solicited-Node Multicast Address Format**



**Note**

There are no broadcast addresses in IPv6. IPv6 multicast addresses are used instead of broadcast addresses.

- [IPv6 Multicast Groups, page 5](#)
- [Scoped Address Architecture, page 5](#)

## IPv6 Multicast Groups

An IPv6 address must be configured on an interface before the interface can 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 FF02:0:0:0:1:FF00::/104 for each unicast and anycast address assigned to the interface



**Note**

The solicited-node multicast address is used in the neighbor discovery process.

- All-nodes link-local multicast group FF02::1
- All-routers link-local multicast group FF02::2

## Scoped Address Architecture

IPv6 includes support for global and nonglobal addresses. This section describes the usage of IPv6 addresses of different scopes.

A scope zone, or a simply a zone, is a connected region of topology of a given scope. For example, the set of links connected by routers within a particular site, and the interfaces attached to those links, comprise a single zone of site-local scope.

A zone is a particular instance of a topological region (for example, Zone1's site or Zone2's site), whereas a scope is the size of a topological region (for example, a site or a link). The zone to which a particular nonglobal address pertains is not encoded in the address itself, but rather is determined by context, such as the interface from which it is sent or received. Therefore, addresses of a given nonglobal scope may be

reused in different zones of that scope. For example, Zone1's site and Zone2's site may each contain a node with site-local address FEC0::1.

Zones of the different scopes are instantiated as follows:

- Each link, and the interfaces attached to that link, comprises a single zone of link-local scope (for both unicast and multicast).
- There is a single zone of global scope (for both unicast and multicast), comprising all the links and interfaces in the Internet.
- The boundaries of zones of scope other than interface-local, link-local, and global must be defined and configured by network administrators. A site boundary serves as such for both unicast and multicast.

Zone boundaries are relatively static features and do not change in response to short-term changes in topology. Therefore, the requirement that the topology within a zone be "connected" is intended to include links and interfaces that may be connected only occasionally. For example, a residential node or network that obtains Internet access by dialup to an employer's site may be treated as part of the employer's site-local zone even when the dialup link is disconnected. Similarly, a failure of a router, interface, or link that causes a zone to become partitioned does not split that zone into multiple zones; rather, the different partitions are still considered to belong to the same zone.

Zones have the following additional properties:

- Zone boundaries cut through nodes, not links (the global zone has no boundary, and the boundary of an interface-local zone encloses just a single interface.)
- Zones of the same scope cannot overlap; that is, they can have no links or interfaces in common.
- A zone of a given scope (less than global) falls completely within zones of larger scope; that is, a smaller scope zone cannot include more topology than any larger scope zone with which it shares any links or interfaces.
- Each interface belongs to exactly one zone of each possible scope.

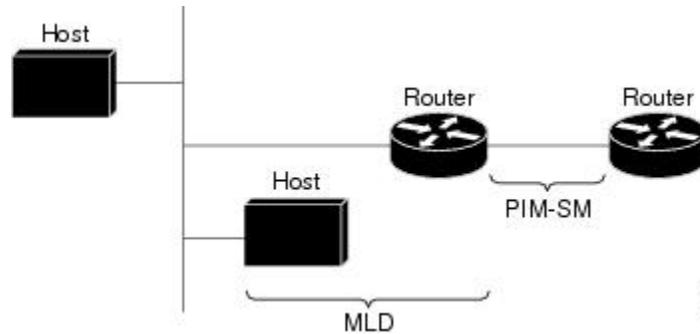
## IPv6 Multicast Routing Implementation

Cisco 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 Internet Group Management Protocol (IGMP) for IPv4, and 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 will interoperate with a router running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM-SM 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 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 3** 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 routers 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, such as a router, that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver, including routers, 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 router alert option set. The router 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 will not be 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 router 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, page 8](#)
- [Explicit Tracking of Receivers, page 8](#)
- [IPv6 Multicast User Authentication and Profile Support, page 8](#)
- [IPv6 MLD Proxy, page 9](#)

## MLD Access Group

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

## Explicit Tracking of Receivers

The explicit tracking feature allows a router to track the behavior of the hosts within its IPv6 network. This feature also enables the fast leave mechanism to be used with MLD version 2 host reports.

## IPv6 Multicast User Authentication and Profile Support

IPv6 multicast by design allows any host in the network to become a receiver or a source for a multicast group. Therefore, multicast access control is needed to control multicast traffic in the network. Access control functionality consists mainly of source access control and accounting, receiver access control and accounting, and provisioning of this access control mechanism.

Multicast access control provides an interface between multicast and authentication, authorization, and accounting (AAA) for provisioning, authorizing, and accounting at the last-hop router, receiver access control functions in multicast, and group or channel disabling capability in multicast.

When you deploy a new multicast service environment, it is necessary to add user authentication and provide a user profile download on a per-interface basis. The use of AAA and IPv6 multicast supports user authentication and downloading of the user profile in a multicast environment.

The event that triggers the download of a multicast access-control profile from the RADIUS server to the access router is arrival of an MLD join on the access router. When this event occurs, a user can cause the

authorization cache to time out and request download periodically or use an appropriate multicast clear command to trigger a new download in case of profile changes.

Accounting occurs via RADIUS accounting. Start and stop accounting records are sent to the RADIUS server from the access router. In order for you to track resource consumption on a per-stream basis, these accounting records provide information about the multicast source and group. The start record is sent when the last-hop router receives a new MLD report, and the stop record is sent upon MLD leave or if the group or channel is deleted for any reason.

## IPv6 MLD Proxy

The MLD proxy feature provides a mechanism for a router to generate MLD membership reports for all (\*, G)/(S, G) entries or a user-defined subset of these entries on the router's upstream interface. The MLD proxy feature enables a device to learn proxy group membership information, and forward multicast packets based upon that information.

If a router is acting as RP for mroute proxy entries, MLD membership reports for these entries can be generated on user specified proxy interface.

## Protocol Independent Multicast

Protocol Independent Multicast (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 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.

You can configure IPv6 multicast to use either PIM-SM or PIM-SSM operation, or you can use both PIM-SM and PIM-SSM together in your network.

- [PIM-Sparse Mode, page 9](#)
- [IPv6 BSR: Configure RP Mapping, page 12](#)
- [PIM-Source Specific Multicast, page 12](#)
- [Routable Address Hello Option, page 15](#)
- [Bidirectional PIM, page 15](#)

## PIM-Sparse Mode

IPv6 multicast provides support for intradomain multicast routing using PIM-SM. PIM-SM uses unicast routing to provide reverse-path information for multicast tree building, but it is not dependent on any particular unicast routing protocol.

PIM-SM is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. PIM-SM initially uses shared trees, which requires the use of an RP.

Requests are accomplished via PIM joins, which are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the RP in the case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups and the hosts that send multicast packets are registered with the RP by that host's first-hop router.

As a PIM join travels up the tree, routers along the path set up multicast forwarding state so that the requested multicast traffic will be forwarded back down the tree. When multicast traffic is no longer

needed, a router sends a PIM prune up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each router updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed. A multicast data sender sends data destined for a multicast group. The designated router (DR) of the sender takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, de-encapsulates them, and forwards them onto the shared tree. The packets then follow the (\*, G) multicast tree state in the routers on the RP tree, being replicated wherever the RP tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulation packets are called PIM register packets.

- [Designated Router, page 10](#)
- [Rendezvous Point, page 11](#)
- [PIMv6 Anycast RP Solution Overview, page 12](#)

## Designated Router

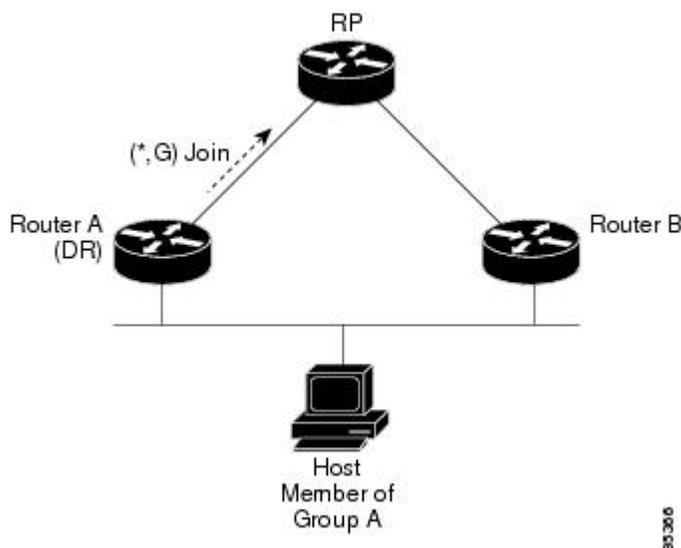
Cisco routers use PIM-SM to forward multicast traffic and follow an election process to select a designated router when there is more than one router on a LAN segment.

The designated router is responsible for sending PIM register and PIM join and prune messages toward the RP to inform it about active sources and host group membership.

If there are multiple PIM-SM routers on a LAN, a designated router must be elected to avoid duplicating multicast traffic for connected hosts. The PIM router with the highest IPv6 address becomes the DR for the LAN unless you choose to force the DR election by use of the **ipv6 pim dr-priority** command. This command allows you to specify the DR priority of each router on the LAN segment (default priority = 1) so that the router with the highest priority will be elected as the DR. If all routers on the LAN segment have the same priority, then the highest IPv6 address is again used as the tiebreaker.

The figure below illustrates what happens on a multiaccess segment. Router A and Router B are connected to a common multiaccess Ethernet segment with Host A as an active receiver for Group A. Only Router A, operating as the DR, sends joins to the RP to construct the shared tree for Group A. If Router B was also permitted to send (\*, G) joins to the RP, parallel paths would be created and Host A would receive duplicate multicast traffic. Once Host A begins to source multicast traffic to the group, the DR's responsibility is to send register messages to the RP. If both routers were assigned the responsibility, the RP would receive duplicate multicast packets.

**Figure 4** Designated Router Election on a Multiaccess Segment



95306

If the DR should fail, the PIM-SM provides a way to detect the failure of Router A and elect a failover DR. If the DR (Router A) became inoperable, Router B would detect this situation when its neighbor adjacency with Router A timed out. Because Router B has been hearing MLD membership reports from Host A, it already has MLD state for Group A on this interface and would immediately send a join to the RP when it became the new DR. This step reestablishes traffic flow down a new branch of the shared tree via Router B. Additionally, if Host A were sourcing traffic, Router B would initiate a new register process immediately after receiving the next multicast packet from Host A. This action would trigger the RP to join the SPT to Host A via a new branch through Router B.

**Tip**

Two PIM routers are neighbors if there is a direct connection between them. To display your PIM neighbors, use the **show ipv6 pim neighbor** command in privileged EXEC mode.

**Note**

The DR election process is required only on multiaccess LANs.

## Rendezvous Point

IPv6 PIM provides embedded RP support. Embedded RP support allows the router to learn RP information using the multicast group destination address instead of the statically configured RP. For routers that are the RP, the router must be statically configured as the RP.

The router searches for embedded RP group addresses in MLD reports or PIM messages and data packets. On finding such an address, the router learns the RP for the group from the address itself. It then uses this learned RP for all protocol activity for the group. For routers that are the RP, the router is advertised as an embedded RP must be configured as the RP.

To select a static RP over an embedded RP, the specific embedded RP group range or mask must be configured in the access list of the static RP. When PIM is configured in sparse mode, you must also choose one or more routers to operate as an RP. An RP is a single common root placed at a chosen point of a shared distribution tree and is configured statically in each box.

PIM DRs forward data from directly connected multicast sources to the RP for distribution down the shared tree. Data is forwarded to the RP in one of two ways:

- Data is encapsulated in register packets and unicast directly to the RP by the first-hop router operating as the DR.
- If the RP has itself joined the source tree, it is multicast-forwarded per the RPF forwarding algorithm described in the PIM-Sparse Mode section.

The RP address is used by first-hop routers to send PIM register messages on behalf of a host sending a packet to the group. The RP address is also used by last-hop routers to send PIM join and prune messages to the RP to inform it about group membership. You must configure the RP address on all routers (including the RP router).

A PIM router can be an RP for more than one group. Only one RP address can be used at a time within a PIM domain for a certain group. The conditions specified by the access list determine for which groups the router is an RP.

IPv6 multicast supports the PIM accept register feature, which is the ability to perform PIM-SM register message filtering at the RP. The user can match an access list or compare the AS path for the registered source with the AS path specified in a route map.

## PIMv6 Anycast RP Solution Overview

The anycast RP solution in IPv6 PIM allows an IPv6 network to support anycast services for the PIM-SM RP. It allows anycast RP to be used inside a domain that runs PIM only. Anycast RP can be used in IPv4 as well as IPv6, but it does not depend on the Multicast Source Discovery Protocol (MSDP), which runs only on IPv4. This feature is useful when interdomain connection is not required.

Anycast RP is a mechanism that ISP-based backbones use to get fast convergence when a PIM RP device fails. To allow receivers and sources to rendezvous to the closest RP, the packets from a source need to get to all RPs to find joined receivers.

A unicast IP address is chosen as the RP address. This address is either statically configured or distributed using a dynamic protocol to all PIM devices throughout the domain. A set of devices in the domain is chosen to act as RPs for this RP address; these devices are called the anycast RP set. Each device in the anycast RP set is configured with a loopback interface using the RP address. Each device in the anycast RP set also needs a separate physical IP address to be used for communication between the RPs.

The RP address, or a prefix that covers the RP address, is injected into the unicast routing system inside of the domain. Each device in the anycast RP set is configured with the addresses of all other devices in the anycast RP set, and this configuration must be consistent in all RPs in the set.

## IPv6 BSR: Configure RP Mapping

PIM routers in a domain must be able to map each multicast group to the correct RP address. The BSR protocol for PIM-SM provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected and the mapping tables will be modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.

Every PIM-SM multicast group needs to be associated with the IP or IPv6 address of an RP. When a new multicast sender starts sending, its local DR will encapsulate these data packets in a PIM register message and send them to the RP for that multicast group. When a new multicast receiver joins, its local DR will send a PIM join message to the RP for that multicast group. When any PIM router sends a (\*, G) join message, the PIM router needs to know which is the next router toward the RP so that G (Group) can send a message to that router. Also, when a PIM router is forwarding data packets using (\*, G) state, the PIM router needs to know which is the correct incoming interface for packets destined for G, because it needs to reject any packets that arrive on other interfaces.

A small set of routers from a domain are configured as candidate bootstrap routers (C-BSRs) and a single BSR is selected for that domain. A set of routers within a domain are also configured as candidate RPs (C-RPs); typically, these routers are the same routers that are configured as C-BSRs. Candidate RPs periodically unicast candidate-RP-advertisement (C-RP-Adv) messages to the BSR of that domain, advertising their willingness to be an RP. A C-RP-Adv message includes the address of the advertising C-RP, and an optional list of group addresses and mask length fields, indicating the group prefixes for which the candidacy is advertised. The BSR then includes a set of these C-RPs, along with their corresponding group prefixes, in bootstrap messages (BSMs) it periodically originates. BSMs are distributed hop-by-hop throughout the domain.

Bidirectional BSR support allows bidirectional RPs to be advertised in C-RP messages and bidirectional ranges in the BSM. All routers in a system must be able to use the bidirectional range in the BSM; otherwise, the bidirectional RP feature will not function.

## 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 routers by MLD membership reports, resulting in shortest-path trees directly to the sources.

In SSM, delivery of datagrams is based on (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 will 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 will run with MLD, SSM must be supported in the Cisco IPv6 router, the host where the application is running, and the application itself.

- [SSM Mapping for IPv6, page 13](#)
- [PIM Shared Tree and Source Tree \(Shortest-Path Tree\), page 13](#)
- [Reverse Path Forwarding, page 15](#)

## SSM 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.

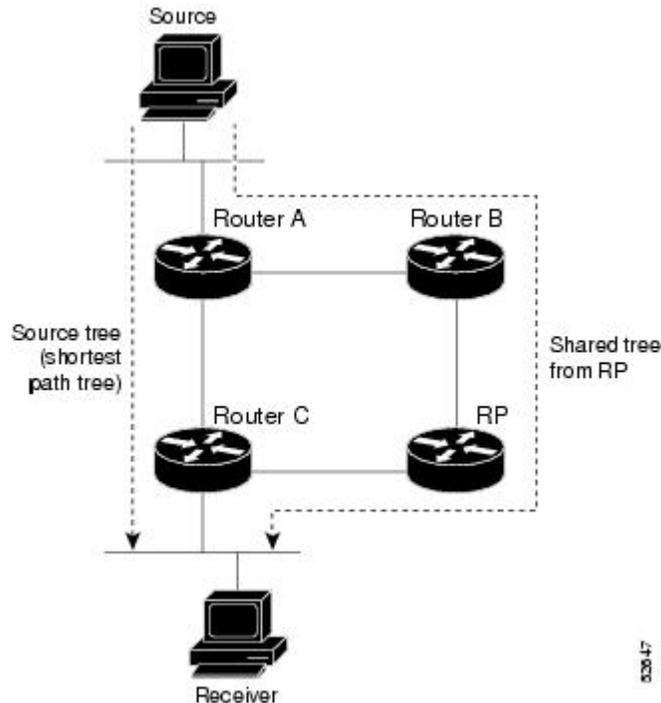
SSM mapping allows the router to look up the source of a multicast MLD version 1 report either in the running configuration of the router or from a DNS server. The router can then initiate an (S, G) join toward the source.

## PIM Shared Tree and Source Tree (Shortest-Path Tree)

By default, members of a group receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called shared tree or rendezvous point tree (RPT), as

illustrated in the figure below. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

**Figure 5** Shared Tree and Source Tree (Shortest Path Tree)



If the data threshold warrants, leaf routers on the shared tree may initiate a switch to the data distribution tree rooted at the source. This type of distribution tree is called a shortest path tree or source tree. By default, the Cisco IOS software switches to a source tree upon receiving the first data packet from a source.

The following process details the move from shared tree to source tree:

- 1 Receiver joins a group; leaf Router C sends a join message toward the RP.
- 2 RP puts the link to Router C in its outgoing interface list.
- 3 Source sends the data; Router A encapsulates the data in the register and sends it to the RP.
- 4 RP forwards the data down the shared tree to Router C and sends a join message toward the source. At this point, data may arrive twice at Router C, once encapsulated and once natively.
- 5 When data arrives natively (unencapsulated) at the RP, the RP sends a register-stop message to Router A.
- 6 By default, receipt of the first data packet prompts Router C to send a join message toward the source.
- 7 When Router C receives data on (S, G), it sends a prune message for the source up the shared tree.
- 8 RP deletes the link to Router C from the outgoing interface of (S, G).
- 9 RP triggers a prune message toward the source.

Join and prune messages are sent for sources and RPs. They are sent hop-by-hop and are processed by each PIM router along the path to the source or RP. Register and register-stop messages are not sent hop-by-hop. They are sent by the designated router that is directly connected to a source and are received by the RP for the group.

## Reverse Path Forwarding

Reverse-path forwarding is used for forwarding multicast datagrams. It functions as follows:

- If a router receives a datagram on an interface it uses to send unicast packets to the source, the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a router forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM uses both source trees and RP-rooted shared trees to forward datagrams; the RPF check is performed differently for each, as follows:

- If a PIM router has source-tree state (that is, an (S, G) entry is present in the multicast routing table), the router performs the RPF check against the IPv6 address of the source of the multicast packet.
- If a PIM router has shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP's address (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S, G) joins (which are source-tree states) are sent toward the source. (\*, G) joins (which are shared-tree states) are sent toward the RP.

## Routable Address Hello Option

When an IPv6 interior gateway protocol is used to build the unicast routing table, the procedure to detect the upstream router address assumes the address of a PIM neighbor is always same as the address of the next-hop router, as long as they refer to the same router. However, it may not be the case when a router has multiple addresses on a link.

Two typical situations can lead to this situation for IPv6. The first situation can occur when the unicast routing table is not built by an IPv6 interior gateway protocol such as multicast BGP. The second situation occurs when the address of an RP shares a subnet prefix with downstream routers (note that the RP router address has to be domain-wide and therefore cannot be a link-local address).

The routable address hello option allows the PIM protocol to avoid such situations by adding a PIM hello message option that includes all the addresses on the interface on which the PIM hello message is advertised. When a PIM router finds an upstream router for some address, the result of RPF calculation is compared with the addresses in this option, in addition to the PIM neighbor's address itself. Because this option includes all the possible addresses of a PIM router on that link, it always includes the RPF calculation result if it refers to the PIM router supporting this option.

Because of size restrictions on PIM messages and the requirement that a routable address hello option fits within a single PIM hello message, a limit of 16 addresses can be configured on the interface.

## Bidirectional PIM

Bidirectional PIM allows multicast routers to keep reduced state information, as compared with unidirectional shared trees in PIM-SM. Bidirectional shared trees convey data from sources to the RPA and distribute them from the RPA to the receivers. Unlike PIM-SM, bidirectional PIM does not switch over to the source tree, and there is no register encapsulation of data from the source to the RP.

A single designated forwarder (DF) exists for each RPA on every link within a bidirectional PIM domain (including multiaccess and point-to-point links). The only exception is the RPL on which no DF exists. The DF is the router on the link with the best route to the RPA, which is determined by comparing MRIB-provided metrics. A DF for a given RPA forwards downstream traffic onto its link and forwards upstream

traffic from its link toward the rendezvous point link (RPL). The DF performs this function for all bidirectional groups that map to the RPA. The DF on a link is also responsible for processing Join messages from downstream routers on the link as well as ensuring that packets are forwarded to local receivers discovered through a local membership mechanism such as MLD.

Bidirectional PIM offers advantages when there are many moderate or low-rate sources. However, the bidirectional shared trees may have worse delay characteristics than do the source trees built in PIM-SM (depending on the topology).

Only static configuration of bidirectional RPs is supported in IPv6.

## Static Mroutes

IPv6 static mroutes behave much in the same way as IPv4 static mroutes used to influence the RPF check. IPv6 static mroutes share the same database as IPv6 static routes and are implemented by extending static route support for RPF checks. Static mroutes support equal-cost multipath mroutes, and they also support unicast-only static routes.

## MRIB

The Multicast Routing Information Base (MRIB) is a protocol-independent repository of multicast routing entries instantiated by multicast routing protocols (routing clients). Its main function is to provide independence between routing protocols and the Multicast Forwarding Information Base (MFIB). It also acts as a coordination and communication point among its clients.

Routing clients use the services provided by the MRIB to instantiate routing entries and retrieve changes made to routing entries by other clients. Besides routing clients, MRIB also has forwarding clients (MFIB instances) and special clients such as MLD. MFIB retrieves its forwarding entries from MRIB and notifies the MRIB of any events related to packet reception. These notifications can either be explicitly requested by routing clients or spontaneously generated by the MFIB.

Another important function of the MRIB is to allow for the coordination of multiple routing clients in establishing multicast connectivity within the same multicast session. MRIB also allows for the coordination between MLD and routing protocols.

## MFIB

The MFIB is a platform-independent and routing-protocol-independent library for IPv6 software. Its main purpose is to provide a Cisco platform with an interface with which to read the IPv6 multicast forwarding table and notifications when the forwarding table changes. The information provided by the MFIB has clearly defined forwarding semantics and is designed to make it easy for the platform to translate to its specific hardware or software forwarding mechanisms.

When routing or topology changes occur in the network, the IPv6 routing table is updated, and those changes are reflected in the MFIB. The MFIB maintains next-hop address information based on the information in the IPv6 routing table. Because there is a one-to-one correlation between MFIB entries and routing table entries, the MFIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths such as fast switching and optimum switching.

- [Distributed MFIB, page 16](#)

## Distributed MFIB

Distributed Multicast Forwarding Information Base (MFIB) is used to switch multicast IPv6 packets on distributed platforms. Distributed MFIB may also contain platform-specific information on replication

across line cards. The basic MFIB routines that implement the core of the forwarding logic are common to all forwarding environments.

dMFIB implements the following functions:

- Distributes a copy of the MFIB to the line cards.
- Relays data-driven protocol events generated in the line cards to PIM.
- Provides an MFIB platform application program interface (API) to propagate MFIB changes to platform-specific code responsible for programming the hardware acceleration engine. This API also includes entry points to switch a packet in software (necessary if the packet is triggering a data-driven event) and to upload traffic statistics to the software.
- Provides hooks to allow clients residing on the RP to read traffic statistics on demand. Distributed MFIB does not periodically upload these statistics to the RP.

The combination of distributed MFIB and MRIB subsystems allows the device to have a "customized" copy of the MFIB database in each line card and to transport MFIB-related platform-specific information from the RP to the line cards.

## 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.

## IPv6 Multicast Process Switching and Fast Switching

A unified MFIB is used to provide both fast switching and process switching support for PIM-SM and PIM-SSM in IPv6 multicast. In process switching, the Route Processor must examine, rewrite, and forward each packet. The packet is first received and copied into the system memory. The router then looks up the Layer 3 network address in the routing table. The Layer 2 frame is then rewritten with the next-hop destination address and sent to the outgoing interface. The RP also computes the cyclic redundancy check (CRC). This switching method is the least scalable method for switching IPv6 packets.

IPv6 multicast fast switching allows routers to provide better packet forwarding performance than process switching. Information conventionally stored in a route cache is stored in several data structures for IPv6 multicast switching. The data structures provide optimized lookup for efficient packet forwarding.

In IPv6 multicast forwarding, the first packet is fast-switched if the PIM protocol logic allows it. In IPv6 multicast fast switching, the MAC encapsulation header is precomputed. IPv6 multicast fast switching uses the MFIB to make IPv6 destination prefix-based switching decisions. In addition to the MFIB, IPv6 multicast fast switching uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all MFIB entries.

The adjacency table is populated as adjacencies are discovered. Each time an adjacency entry is created (such as through ARP), a link-layer header for that adjacent node is precomputed and stored in the adjacency table. Once a route is determined, it points to a next hop and corresponding adjacency entry. It is subsequently used for encapsulation during switching of packets.

A route might have several paths to a destination prefix, such as when a router is configured for simultaneous load balancing and redundancy. For each resolved path, a pointer is added for the adjacency

corresponding to the next-hop interface for that path. This mechanism is used for load balancing across several paths.

## Multiprotocol BGP for the IPv6 Multicast Address Family

The multiprotocol BGP for the IPv6 multicast address family feature provides multicast BGP extensions for IPv6 and supports the same features and functionality as IPv4 BGP. IPv6 enhancements to multicast BGP include support for an IPv6 multicast address family and network layer reachability information (NLRI) and next hop (the next router in the path to the destination) attributes that use IPv6 addresses.

Multicast BGP is an enhanced BGP that allows the deployment of interdomain IPv6 multicast. Multiprotocol BGP carries routing information for multiple network layer protocol address families; for example, IPv6 address family and for IPv6 multicast routes. The IPv6 multicast address family contains routes used for RPF lookup by the IPv6 PIM protocol, and multicast BGP IPv6 provides for interdomain transport of the same. Users must use multiprotocol BGP for IPv6 multicast when using IPv6 multicast with BGP because the unicast BGP learned routes will not be used for IPv6 multicast.

Multicast BGP functionality is provided through a separate address family context. A subsequent address family identifier (SAFI) provides information about the type of the network layer reachability information that is carried in the attribute. Multiprotocol BGP unicast uses SAFI 1 messages, and multiprotocol BGP multicast uses SAFI 2 messages. SAFI 1 messages indicate that the routes are usable only for IP unicast, not IP multicast. Because of this functionality, BGP routes in the IPv6 unicast RIB must be ignored in the IPv6 multicast RPF lookup.

A separate BGP routing table is maintained to configure incongruent policies and topologies (for example, IPv6 unicast and multicast) by using IPv6 multicast RPF lookup. Multicast RPF lookup is very similar to the IP unicast route lookup.

No MRIB is associated with the IPv6 multicast BGP table. However, IPv6 multicast BGP operates on the unicast IPv6 RIB when needed. Multicast BGP does not insert or update routes into the IPv6 unicast RIB.

## NSF and SSO Support In IPv6 Multicast

Support for nonstop forwarding (NSF) and stateful switchover (SSO) is provided in IPv6 Multicast.

## Bandwidth-Based CAC for IPv6 Multicast

The bandwidth-based call admission control (CAC) for IPv6 multicast feature implements a way to count per-interface mroute state limiters using cost multipliers. This feature can be used to provide bandwidth-based CAC on a per-interface basis in network environments where the multicast flows use different amounts of bandwidth.

This feature limits and accounts for IPv6 multicast state in detail. When this feature is configured, interfaces can be limited to the number of times they may be used as incoming or outgoing interfaces in the IPv6 multicast PIM topology.

With this feature, router administrators can configure global limit cost commands for state matching access lists and specify which cost multiplier to use when accounting such state against the interface limits. This feature provides the required flexibility to implement bandwidth-based local CAC policy by tuning appropriate cost multipliers for different bandwidth requirements.

## How to Implement IPv6 Multicast

- [Enabling IPv6 Multicast Routing, page 19](#)
- [Customizing and Verifying the MLD Protocol, page 19](#)
- [Configuring PIM, page 31](#)
- [Configuring a BSR, page 39](#)
- [Configuring SSM Mapping, page 44](#)
- [Configuring Static Mroutes, page 46](#)
- [Configuring IPv6 Multiprotocol BGP, page 47](#)
- [Configuring Bandwidth-Based CAC for IPv6, page 57](#)
- [Using MFIB in IPv6 Multicast, page 60](#)
- [Disabling Default Features in IPv6 Multicast, page 63](#)

## Enabling IPv6 Multicast Routing

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 multicast-routing [vrf vrf-name]`

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>ipv6 multicast-routing [vrf vrf-name]</code>  <b>Example:</b> <pre>Router(config)# ipv6 multicast-routing</pre>	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the router.

## Customizing and Verifying the MLD Protocol

- [Customizing and Verifying MLD on an Interface, page 20](#)
- [Implementing MLD Group Limits, page 22](#)
- [Configuring Explicit Tracking of Receivers to Track Host Behavior, page 24](#)

- [Configuring Multicast User Authentication and Profile Support, page 25](#)
- [Enabling MLD Proxy in IPv6, page 28](#)
- [Resetting the MLD Traffic Counters, page 30](#)
- [Clearing the MLD Interface Counters, page 31](#)

## Customizing and Verifying MLD on an Interface

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]}
5. **ipv6 mld access-group** *access-list-name*
6. **ipv6 mld static-group** *group-address* ] [**include**| **exclude**] {*source-address* | **source-list** [*acl*]}
7. **ipv6 mld query-max-response-time** *seconds*
8. **ipv6 mld query-timeout** *seconds*
9. **ipv6 mld query-interval** *seconds*
10. **exit**
11. **show ipv6 mld** [*vrf vrf-name*] **groups** [**link-local**] [*group-name* | *group-address*] [*interface-type* *interface-number*] [**detail** | **explicit**]
12. **show ipv6 mld groups summary**
13. **show ipv6 mld** [*vrf vrf-name*] **interface** [*type number*]
14. **debug ipv6 mld** [*group-name* | *group-address* | *interface-type*]
15. **debug ipv6 mld explicit** [*group-name* | *group-address*]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b></p> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	<p><b>ipv6 mld join-group</b> [<i>group-address</i>] [<b>include</b>   <b>exclude</b>] {<i>source-address</i>   <b>source-list</b> [<i>acl</i>]}</p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 mld join-group FF04::10</pre>	Configures MLD reporting for a specified group and source.
Step 5	<p><b>ipv6 mld access-group</b> <i>access-list-name</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 access-list acc-grp-1</pre>	Allows the user to perform IPv6 multicast receiver access control.
Step 6	<p><b>ipv6 mld static-group</b> <i>group-address</i> ] [<b>include</b>   <b>exclude</b>] {<i>source-address</i>   <b>source-list</b> [<i>acl</i>]}</p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 mld static-group ff04::10 include 100::1</pre>	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.
Step 7	<p><b>ipv6 mld query-max-response-time</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 mld query-max-response-time 20</pre>	Configures the maximum response time advertised in MLD queries.
Step 8	<p><b>ipv6 mld query-timeout</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 mld query-timeout 130</pre>	Configures the timeout value before the router takes over as the querier for the interface.
Step 9	<p><b>ipv6 mld query-interval</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 mld query-interval 60</pre>	<p>Configures the frequency at which the Cisco IOS software sends MLD host-query messages.</p> <p><b>Caution</b> Changing this value may severely impact multicast forwarding.</p>

Command or Action	Purpose
<b>Step 10</b> <code>exit</code>  <b>Example:</b> <pre>Router(config-if)# exit</pre>	Enter this command twice to exit interface configuration mode and enter privileged EXEC mode.
<b>Step 11</b> <code>show ipv6 mld [vrf vrf-name] groups [link-local] [group-name   group-address] [interface-type interface-number] [detail   explicit]</code>  <b>Example:</b> <pre>Router# show ipv6 mld groups FastEthernet 2/1</pre>	Displays the multicast groups that are directly connected to the router and that were learned through MLD.
<b>Step 12</b> <code>show ipv6 mld groups summary</code>  <b>Example:</b> <pre>Router# show ipv6 mld groups summary</pre>	Displays the number of (*, G) and (S, G) membership reports present in the MLD cache.
<b>Step 13</b> <code>show ipv6 mld [vrf vrf-name] interface [type number]</code>  <b>Example:</b> <pre>Router# show ipv6 mld interface FastEthernet 2/1</pre>	Displays multicast-related information about an interface.
<b>Step 14</b> <code>debug ipv6 mld [group-name   group-address   interface-type]</code>  <b>Example:</b> <pre>Router# debug ipv6 mld</pre>	Enables debugging on MLD protocol activity.
<b>Step 15</b> <code>debug ipv6 mld explicit [group-name   group-address]</code>  <b>Example:</b> <pre>Router# debug ipv6 mld explicit</pre>	Displays information related to the explicit tracking of hosts.

## Implementing MLD Group Limits

Per-interface and global MLD limits operate independently of each other. Both per-interface and global MLD limits can be configured on the same router. The number of MLD limits, globally or per interface, is not configured by default; the limits must be configured by the user. A membership report that exceeds either the per-interface or the global state limit is ignored.

- [Implementing MLD Group Limits Globally, page 23](#)
- [Implementing MLD Group Limits per Interface, page 23](#)

## Implementing MLD Group Limits Globally

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mld [vrf *vrf-name*] state-limit *number***

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 mld [vrf <i>vrf-name</i>] state-limit <i>number</i></b>  <b>Example:</b> Router(config)# ipv6 mld state-limit 300	Limits the number of MLD states globally.

## Implementing MLD Group Limits per Interface

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ipv6 mld limit *number* [except *access-list***

## DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>interface type number</code>  <b>Example:</b> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 4</b> <code>ipv6 mld limit number [except access-list]</code>  <b>Example:</b> <pre>Router(config-if)# ipv6 mld limit 100</pre>	Limits the number of MLD states on a per-interface basis.

## Configuring Explicit Tracking of Receivers to Track Host Behavior

The explicit tracking feature allows a router to track the behavior of the hosts within its IPv6 network and enables the fast leave mechanism to be used with MLD version 2 host reports.

### SUMMARY STEPS

- `enable`
- `configure terminal`
- `interface type number`
- `ipv6 mld explicit-tracking access-list-name`

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>interface type number</code>  <b>Example:</b> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 4</b> <code>ipv6 mld explicit-tracking access-list-name</code>  <b>Example:</b> <pre>Router(config-if)# ipv6 mld explicit-tracking list1</pre>	Enables explicit tracking of hosts.

**Configuring Multicast User Authentication and Profile Support**

- [Prerequisites, page 25](#)
- [Restrictions, page 25](#)
- [Enabling AAA Access Control for IPv6 Multicast, page 26](#)
- [Specifying Method Lists and Enabling Multicast Accounting, page 26](#)
- [Disabling the Router from Receiving Unauthenticated Multicast Traffic, page 28](#)

**Prerequisites**

Before you configure multicast user authentication and profile support, you may configure the following receiver access control functions in IPv6 multicast.

**Restrictions**

Before you configure multicast user authentication and profile support, you should be aware of the following restrictions:

- The port, interface, VC, or VLAN ID is the user or subscriber identity. User identity by hostname, user ID, or password is not supported.

- [Enabling AAA Access Control for IPv6 Multicast, page 26](#)
- [Specifying Method Lists and Enabling Multicast Accounting, page 26](#)
- [Disabling the Router from Receiving Unauthenticated Multicast Traffic, page 28](#)
- [Resetting Authorization Status on an MLD Interface, page 29](#)

## Enabling AAA Access Control for IPv6 Multicast

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router(config)# aaa new-model	Enables the AAA access control system.

## Specifying Method Lists and Enabling Multicast Accounting

Perform this task to specify the method lists used for AAA authorization and accounting and how to enable multicast accounting on specified groups or channels on an interface.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **aaa authorization multicast default** *[method3 | method4]*
4. **aaa accounting multicast default** **[start-stop | stop-only]** **[broadcast]** *[method1] [method2] [method3] [method4]*
5. **interface** *type number*
6. **ipv6 multicast aaa account receive** *access-list-name* **[throttle** *throttle-number*

**DETAILED STEPS**

Command or Action	Purpose
<p><b>Step 1</b> <b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <b>aaa authorization multicast default</b> <i>[method3   method4]</i></p> <p><b>Example:</b></p> <pre>Router(config)# aaa authorization multicast default</pre>	<p>Enables AAA authorization and sets parameters that restrict user access to an IPv6 multicast network.</p>
<p><b>Step 4</b> <b>aaa accounting multicast default</b> <b>[start-stop   stop-only]</b> <b>[broadcast]</b> <i>[method1] [method2] [method3] [method4]</i></p> <p><b>Example:</b></p> <pre>Router(config)# aaa accounting multicast default</pre>	<p>Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.</p>
<p><b>Step 5</b> <b>interface</b> <i>type number</i></p> <p><b>Example:</b></p> <pre>Router(config)# interface FastEthernet 1/0</pre>	<p>Specifies an interface type and number, and places the router in interface configuration mode.</p>

Command or Action	Purpose
<b>Step 6</b> <code>ipv6 multicast aaa account receive <i>access-list-name</i> [throttle <i>throttle-number</i>]</code>  <b>Example:</b>  <pre>Router(config-if)# ipv6 multicast aaa account receive list1</pre>	Enables AAA accounting on specified groups or channels.

### Disabling the Router from Receiving Unauthenticated Multicast Traffic

In some situations, access control may be needed to prevent multicast traffic from being received unless the subscriber is authenticated and the channels are authorized as per access control profiles. That is, there should be no traffic at all unless specified otherwise by access control profiles.

Perform this task to disable the router from receiving multicast traffic to be received from unauthenticated groups or unauthorized channels.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 multicast [vrf vrf-name] group-range[access-list-name]`

#### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b>  <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b>  <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>ipv6 multicast [vrf <i>vrf-name</i>] group-range[<i>access-list-name</i>]</code>  <b>Example:</b>  <pre>Router(config)# ipv6 multicast group-range</pre>	Disables multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router.

### Enabling MLD Proxy in IPv6

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 mld host-proxy** [*group-acl*]
4. **ipv6 mld host-proxy interface** [*group-acl*]
5. **show ipv6 mld host-proxy** [*interface-type interface-number*] **group** [*group-address*]]

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1 enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2 configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3 ipv6 mld host-proxy</b> [ <i>group-acl</i> ]  <b>Example:</b> Router(config)# ipv6 mld host-proxy proxy-group	Enables the MLD proxy feature.
<b>Step 4 ipv6 mld host-proxy interface</b> [ <i>group-acl</i> ]  <b>Example:</b> Router(config)# ipv6 mld host-proxy interface Ethernet 0/0	Enables the MLD proxy feature on a specified interface on an RP.
<b>Step 5 show ipv6 mld host-proxy</b> [ <i>interface-type interface-number</i> ] <b>group</b> [ <i>group-address</i> ]]  <b>Example:</b> Router# show ipv6 mld host-proxy Ethernet0/0	Displays IPv6 MLD host proxy information.

- [Resetting Authorization Status on an MLD Interface, page 29](#)

**Resetting Authorization Status on an MLD Interface**

If no interface is specified, authorization is reset on all MLD interfaces.

**SUMMARY STEPS**

1. enable
2. clear ipv6 multicast aaa authorization [*interface-type interface-number*]

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> enable  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> clear ipv6 multicast aaa authorization [ <i>interface-type interface-number</i> ]  <b>Example:</b> <pre>Router# clear ipv6 multicast aaa authorization FastEthernet 1/0</pre>	Clears parameters that restrict user access to an IPv6 multicast network.

**Resetting the MLD Traffic Counters****SUMMARY STEPS**

1. enable
2. clear ipv6 mld [*vrf vrf-name*] traffic
3. show ipv6 mld [*vrf vrf-name*] traffic

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> enable  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> clear ipv6 mld [ <i>vrf vrf-name</i> ] traffic  <b>Example:</b> <pre>Router# clear ipv6 mld traffic</pre>	Resets all MLD traffic counters.

	Command or Action	Purpose
Step 3	<pre>show ipv6 mld [vrf vrf-name] traffic</pre> <p><b>Example:</b></p> <pre>Router# show ipv6 mld traffic</pre>	Displays the MLD traffic counters.

## Clearing the MLD Interface Counters

### SUMMARY STEPS

1. enable
2. clear ipv6 mld [vrf vrf-name] counters interface-type

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>clear ipv6 mld [vrf vrf-name] counters interface-type</pre> <p><b>Example:</b></p> <pre>Router# clear ipv6 mld counters Ethernet1/0</pre>	Clears the MLD interface counters.

## Configuring PIM

- [Configuring PIM-SM and Displaying PIM-SM Information for a Group Range, page 31](#)
- [Configuring PIM Options, page 33](#)
- [Configuring Bidirectional PIM and Displaying Bidirectional PIM Information, page 35](#)
- [Resetting the PIM Traffic Counters, page 37](#)
- [Clearing the PIM Topology Table to Reset the MRIB Connection, page 37](#)

### Configuring PIM-SM and Displaying PIM-SM Information for a Group Range

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]**
4. **exit**
5. **show ipv6 pim [vrf vrf-name] interface [state-on] [state-off] [type number]**
6. **show ipv6 pim [vrf vrf-name] group-map [group-name | group-address] | [group-range | group-mask] [info-source {bsr | default | embedded-rp | static}]**
7. **show ipv6 pim [vrf vrf-name] neighbor [detail] [interface-type interface-number | count]**
8. **show ipv6 pim [vrf vrf-name] range-list[config] [rp-address | rp-name]**
9. **show ipv6 pim [vrf vrf-name] tunnel [interface-type interface-number]**
10. **debug ipv6 pim [group-name | group-address | interface interface-type | bsr | group | mvpn | neighbor]**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]</b>  <b>Example:</b> Router(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1	Configures the address of a PIM RP for a particular group range.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits global configuration mode, and returns the router to privileged EXEC mode.

	Command or Action	Purpose
Step 5	<p><b>show ipv6 pim</b> [<b>vrf</b> <i>vrf-name</i>] <b>interface</b> [<b>state-on</b>] [<b>state-off</b>] [<i>type number</i>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim interface</pre>	Displays information about interfaces configured for PIM.
Step 6	<p><b>show ipv6 pim</b> [<b>vrf</b> <i>vrf-name</i>] <b>group-map</b> [<i>group-name</i>   <i>group-address</i>]   [<i>group-range</i>   <i>group-mask</i>] [<b>info-source</b> {<b>bsr</b>   <b>default</b>   <b>embedded-rp</b>   <b>static</b>}]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim group-map</pre>	Displays an IPv6 multicast group mapping table.
Step 7	<p><b>show ipv6 pim</b> [<b>vrf</b> <i>vrf-name</i>] <b>neighbor</b> [<b>detail</b>] [<i>interface-type interface-number</i>   <b>count</b>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim neighbor</pre>	Displays the PIM neighbors discovered by the Cisco IOS software.
Step 8	<p><b>show ipv6 pim</b> [<b>vrf</b> <i>vrf-name</i>] <b>range-list</b>[<b>config</b>] [<i>rp-address</i>   <i>rp-name</i>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim range-list</pre>	Displays information about IPv6 multicast range lists.
Step 9	<p><b>show ipv6 pim</b> [<b>vrf</b> <i>vrf-name</i>] <b>tunnel</b> [<i>interface-type interface-number</i>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim tunnel</pre>	Displays information about the PIM register encapsulation and de-encapsulation tunnels on an interface.
Step 10	<p><b>debug ipv6 pim</b> [<i>group-name</i>   <i>group-address</i>] <b>interface</b> <i>interface-type</i>   <b>bsr</b>   <b>group</b>   <b>mvpn</b>   <b>neighbor</b>]</p> <p><b>Example:</b></p> <pre>Router# debug ipv6 pim</pre>	Enables debugging on PIM protocol activity.

## Configuring PIM Options

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 pim [vrf vrf-name] spt-threshold infinity [group-list access-list-name]**
4. **ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}**
5. **interface type number**
6. **ipv6 pim dr-priority value**
7. **ipv6 pim hello-interval seconds**
8. **ipv6 pim join-prune-interval seconds**
9. **exit**
10. **show ipv6 pim [vrf vrf-name] join-prune statistic [interface-type]**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<b>Step 3</b>	<p><b>ipv6 pim [vrf vrf-name] spt-threshold infinity [group-list access-list-name]</b></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1</pre>	<p>Configures when a PIM leaf router joins the SPT for the specified groups.</p>
<b>Step 4</b>	<p><b>ipv6 pim [vrf vrf-name] accept-register {list access-list   route-map map-name}</b></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim accept-register route-map reg-filter</pre>	<p>Accepts or rejects registers at the RP.</p>

	Command or Action	Purpose
<b>Step 5</b>	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b></p> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 6</b>	<p><b>ipv6 pim dr-priority</b> <i>value</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 pim dr-priority 3</pre>	Configures the DR priority on a PIM router.
<b>Step 7</b>	<p><b>ipv6 pim hello-interval</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 pim hello-interval 45</pre>	Configures the frequency of PIM hello messages on an interface.
<b>Step 8</b>	<p><b>ipv6 pim join-prune-interval</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 pim join-prune-interval 75</pre>	Configures periodic join and prune announcement intervals for a specified interface.
<b>Step 9</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Enter this command twice to exit interface configuration mode and enter privileged EXEC mode.
<b>Step 10</b>	<p><b>show ipv6 pim</b> [<b>vrf</b> <i>vrf-name</i>] <b>join-prune statistic</b> [<i>interface-type</i>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim join-prune statistic</pre>	Displays the average join-prune aggregation for the most recently aggregated packets for each interface.

## Configuring Bidirectional PIM and Displaying Bidirectional PIM Information

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]**
4. **exit**
5. **show ipv6 pim [vrf vrf-name] df [interface-type interface-number] [rp-address]**
6. **show ipv6 pim [vrf vrf-name] df winner[interface-type interface-number] [rp-address]**

**DETAILED STEPS**

Command or Action	Purpose
<p><b>Step 1</b> <b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <b>ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]</b></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C bidir</pre>	<p>Configures the address of a PIM RP for a particular group range. Use of the <b>bidir</b> keyword means that the group range will be used for bidirectional shared-tree forwarding.</p>
<p><b>Step 4</b> <b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	<p>Exits global configuration mode, and returns the router to privileged EXEC mode.</p>
<p><b>Step 5</b> <b>show ipv6 pim [vrf vrf-name] df [interface-type interface-number] [rp-address]</b></p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim df</pre>	<p>Displays the designated forwarder (DF)-election state of each interface for RP.</p>

Command or Action	Purpose
<p><b>Step 6</b> <code>show ipv6 pim [vrf vrf-name] df winner[interface-type interface-number] [rp-address]</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim df winner ethernet 1/0 200::1</pre>	<p>Displays the DF-election winner on each interface for each RP.</p>

## Resetting the PIM Traffic Counters

If PIM malfunctions or in order to verify that the expected number of PIM packets are received and sent, the user can clear PIM traffic counters. Once the traffic counters are cleared, the user can enter the **show ipv6 pim traffic** command to verify that PIM is functioning correctly and that PIM packets are being received and sent correctly.

### SUMMARY STEPS

1. **enable**
2. **clear ipv6 pim [vrf vrf-name] traffic**
3. **show ipv6 pim [vrf vrf-name] traffic**

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>clear ipv6 pim [vrf vrf-name] traffic</code></p> <p><b>Example:</b></p> <pre>Router# clear ipv6 pim traffic</pre>	<p>Resets the PIM traffic counters.</p>
<p><b>Step 3</b> <code>show ipv6 pim [vrf vrf-name] traffic</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim traffic</pre>	<p>Displays the PIM traffic counters.</p>

## Clearing the PIM Topology Table to Reset the MRIB Connection

No configuration is necessary to use the MRIB. However, users may in certain situations want to clear the PIM topology table in order to reset the MRIB connection and verify MRIB information.

**SUMMARY STEPS**

1. **enable**
2. **clear ipv6 pim** [*vrf vrf-name*] **topology** [*group-name* | *group-address*]
3. **show ipv6 mrib** [*vrf vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* : *client-id*}]
4. **show ipv6 mrib** [*vrf vrf-name*] **route** [**link-local** | **summary**] | [*sourceaddress-or-name* | \*] [*groupname-or-address* [*prefix-length*]]
5. **show ipv6 pim** [*vrf vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]]
6. **debug ipv6 mrib** [*vrf vrf-name*] **client**
7. **debug ipv6 mrib** [*vrf vrf-name*] **io**
8. **debug ipv6 mrib proxy**
9. **debug ipv6 mrib** [*vrf vrf-name*] **route** [*group-name* | *group-address*]
10. **debug ipv6 mrib** [*vrf vrf-name*] **table**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>clear ipv6 pim</b> [ <i>vrf vrf-name</i> ] <b>topology</b> [ <i>group-name</i>   <i>group-address</i> ]  <b>Example:</b>  Router# clear ipv6 pim topology FF04::10	Clears the PIM topology table.
<b>Step 3</b>	<b>show ipv6 mrib</b> [ <i>vrf vrf-name</i> ] <b>client</b> [ <b>filter</b> ] [ <b>name</b> { <i>client-name</i>   <i>client-name</i> : <i>client-id</i> }]  <b>Example:</b>  Router# show ipv6 mrib client	Displays multicast-related information about an interface.
<b>Step 4</b>	<b>show ipv6 mrib</b> [ <i>vrf vrf-name</i> ] <b>route</b> [ <b>link-local</b>   <b>summary</b> ]   [ <i>sourceaddress-or-name</i>   *] [ <i>groupname-or-address</i> [ <i>prefix-length</i> ]]  <b>Example:</b>  Router# show ipv6 mrib route	Displays the MRIB route information.

	Command or Action	Purpose
<b>Step 5</b>	<p><b>show ipv6 pim</b> [<b>vrf vrf-name</b>] <b>topology</b> [<i>groupname-or-address</i>   <i>sourcename-or-address</i>]   <b>link-local</b>   <b>route-count</b> [<b>detail</b>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim topology</pre>	Displays PIM topology table information for a specific group or all groups.
<b>Step 6</b>	<p><b>debug ipv6 mrib</b> [<b>vrf vrf-name</b>] <b>client</b></p> <p><b>Example:</b></p> <pre>Router# debug ipv6 mrib client</pre>	Enables debugging on MRIB client management activity.
<b>Step 7</b>	<p><b>debug ipv6 mrib</b> [<b>vrf vrf-name</b>] <b>io</b></p> <p><b>Example:</b></p> <pre>Router# debug ipv6 mrib io</pre>	Enables debugging on MRIB I/O events.
<b>Step 8</b>	<p><b>debug ipv6 mrib proxy</b></p> <p><b>Example:</b></p> <pre>Router# debug ipv6 mrib proxy</pre>	Enables debugging on MRIB proxy activity between the route processor and line cards on distributed router platforms.
<b>Step 9</b>	<p><b>debug ipv6 mrib</b> [<b>vrf vrf-name</b>] <b>route</b> [<i>group-name</i>   <i>group-address</i>]</p> <p><b>Example:</b></p> <pre>Router# debug ipv6 mrib route</pre>	Displays information about MRIB routing entry-related activity.
<b>Step 10</b>	<p><b>debug ipv6 mrib</b> [<b>vrf vrf-name</b>] <b>table</b></p> <p><b>Example:</b></p> <pre>Router# debug ipv6 mrib table</pre>	Enables debugging on MRIB table management activity.

## Configuring a BSR

- [Configuring a BSR and Verifying BSR Information, page 40](#)
- [Sending PIM RP Advertisements to the BSR, page 41](#)
- [Configuring BSR for Use Within Scoped Zones, page 42](#)
- [Configuring BSR Routers to Announce Scope-to-RP Mappings, page 43](#)

## Configuring a BSR and Verifying BSR Information

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim [vrf vrf-name] bsr candidate bsr ipv6-address[hash-mask-length] [priority priority-value]**
4. **interface type number**
5. **ipv6 pim bsr border**
6. **exit**
7. **show ipv6 pim [vrf vrf-name] bsr {election | rp-cache | candidate-rp}**

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <b>ipv6 pim [vrf vrf-name] bsr candidate bsr ipv6-address[hash-mask-length] [priority priority-value]</b></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10</pre>	<p>Configures a router to be a candidate BSR.</p>
<p><b>Step 4</b> <b>interface type number</b></p> <p><b>Example:</b></p> <pre>Router(config)# interface FastEthernet 1/0</pre>	<p>Specifies an interface type and number, and places the router in interface configuration mode.</p>
<p><b>Step 5</b> <b>ipv6 pim bsr border</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 pim bsr border</pre>	<p>Configures a border for all BSMs of any scope on a specified interface.</p>

Command or Action	Purpose
<p><b>Step 6</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Enter this command twice to exit interface configuration mode and enter privileged EXEC mode.
<p><b>Step 7</b> <code>show ipv6 pim [vrf vrf-name] bsr {election   rp-cache   candidate-rp}</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 pim bsr election</pre>	Displays information related to PIM BSR protocol processing.

## Sending PIM RP Advertisements to the BSR

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 pim [vrf vrf-name] bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] [scope scope-value] [bidir]`
4. `interface type number`
5. `ipv6 pim bsr border`

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
<p><b>Step 3</b> <code>ipv6 pim [vrf vrf-name] bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] [scope scope-value] [bidir]</code></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0</pre>	Sends PIM RP advertisements to the BSR.
<p><b>Step 4</b> <code>interface type number</code></p> <p><b>Example:</b></p> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<p><b>Step 5</b> <code>ipv6 pim bsr border</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 pim bsr border</pre>	Configures a border for all BSMs of any scope on a specified interface.

## Configuring BSR for Use Within Scoped Zones

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 pim [vrf vrf-name] bsr candidate bsr ipv6-address [hash-mask-length] [priority priority-value]`
4. `ipv6 pim [vrf vrf-name] bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] [scope scope-value] [bidir]`
5. `interface type number`
6. `ipv6 multicast boundary scope scope-value`

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

Command or Action	Purpose
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <code>ipv6 pim [vrf vrf-name] bsr candidate bsr ipv6-address [hash-mask-length] [priority priority-value]</code></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4</pre>	<p>Configures a router to be a candidate BSR.</p>
<p><b>Step 4</b> <code>ipv6 pim [vrf vrf-name] bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] [scope scope-value] [bidir]</code></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6</pre>	<p>Configures the candidate RP to send PIM RP advertisements to the BSR.</p>
<p><b>Step 5</b> <code>interface type number</code></p> <p><b>Example:</b></p> <pre>Router(config)# interface FastEthernet 1/0</pre>	<p>Specifies an interface type and number, and places the router in interface configuration mode.</p>
<p><b>Step 6</b> <code>ipv6 multicast boundary scope scope-value</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# ipv6 multicast boundary scope 6</pre>	<p>Configures a multicast boundary on the interface for a specified scope.</p>

## Configuring BSR Routers to Announce Scope-to-RP Mappings

IPv6 BSR routers can be statically configured to announce scope-to-RP mappings directly instead of learning them from candidate-RP messages. A user might want to configure a BSR router to announce scope-to-RP mappings so that an RP that does not support BSR is imported into the BSR. Enabling this feature also allows an RP positioned outside the enterprise's BSR domain to be learned by the known remote RP on the local candidate BSR routers.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 pim [vrf vrf-name] bsr announced rp ipv6-address [group-list access-list-name] [priority priority-value] [bidir] [scope scope-value]**

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1 enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2 configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3 ipv6 pim [vrf vrf-name] bsr announced rp ipv6-address [group-list access-list-name] [priority priority-value] [bidir] [scope scope-value]</b>  <b>Example:</b> Router(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0	Announces scope-to-RP mappings directly from the BSR for the specified candidate RP.

**Configuring SSM Mapping**

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

You can use either DNS-based or static SSM mapping, depending on your router 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 will be used.

**Note**

To use DNS-based SSM mapping, the router needs to find at least one correctly configured DNS server, to which the router may be directly attached.

>

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 mld [vrf vrf-name] ssm-map enable**
4. **no ipv6 mld [vrf vrf-name] ssm-map query dns**
5. **ipv6 mld [vrf vrf-name] ssm-map static access-list source-address**
6. **exit**
7. **show ipv6 mld [vrf vrf-name] ssm-map [source-address]**

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>ipv6 mld [vrf vrf-name] ssm-map enable</b>  <b>Example:</b> Router(config)# ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
<b>Step 4</b> <b>no ipv6 mld [vrf vrf-name] ssm-map query dns</b>  <b>Example:</b> Router(config)# no ipv6 mld ssm-map query dns	Disables DNS-based SSM mapping.
<b>Step 5</b> <b>ipv6 mld [vrf vrf-name] ssm-map static access-list source-address</b>  <b>Example:</b> Router(config)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1	Configures static SSM mappings.

Command or Action	Purpose
<b>Step 6</b> <code>exit</code>  <b>Example:</b> <pre>Router(config-if)# exit</pre>	Exits global configuration mode, and returns the router to privileged EXEC mode.
<b>Step 7</b> <code>show ipv6 mld [vrf vrf-name] ssm-map [source-address]</code>  <b>Example:</b> <pre>Router# show ipv6 mld ssm-map</pre>	Displays SSM mapping information.

## Configuring Static Mroutes

Static multicast routes (mroutes) in IPv6 can be implemented as an extension of IPv6 static routes. You can configure your router to use a static route for unicast routing only, to use a static multicast route for multicast RPF selection only, or to use a static route for both unicast routing and multicast RPF selection.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 route** *ipv6-prefix / prefix-length ipv6-address | interface-type interface-number ipv6-address* *[administrative-distance] [administrative-multicast-distance | unicast| multicast] [tag tag]*
4. **exit**
5. **show ipv6 mroute** *[vrf vrf-name] [link-local | group-name | group-address [source-address | source-name]] [summary] [count]*
6. **show ipv6 mroute** *[vrf vrf-name] [link-local | group-name | group-address] active[kbps]*
7. **show ipv6 rpf** *[vrf vrf-name] ipv6-prefix*

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

Command or Action	Purpose
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<p><b>Step 3</b> <code>ipv6 route ipv6-prefix / prefix-length ipv6-address   interface-type interface-number ipv6-address} [administrative-distance] [administrative-multicast-distance   <b>unicast</b>  <b>multicast</b>] [tag tag</code></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 route 2001:DB8::/64 6::6 100</pre>	Establishes static IPv6 routes. The example shows a static route used for both unicast routing and multicast RPF selection.
<p><b>Step 4</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Exits global configuration mode, and returns the router to privileged EXEC mode.
<p><b>Step 5</b> <code>show ipv6 mroute [vrf vrf-name] [link-local   [group-name   group-address [source-address   source-name]] [summary] [count]</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 mroute ff07::1</pre>	Displays the contents of the IPv6 multicast routing table.
<p><b>Step 6</b> <code>show ipv6 mroute [vrf vrf-name] [link-local   group-name   group-address] active[kbps]</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 mroute active</pre>	Displays the active multicast streams on the router.
<p><b>Step 7</b> <code>show ipv6 rpf [vrf vrf-name] ipv6-prefix</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 rpf 2001:DB8::1:1:2</pre>	Checks RPF information for a given unicast host address and prefix.

## Configuring IPv6 Multiprotocol BGP

- [Configuring an IPv6 Peer Group to Perform Multicast BGP Routing, page 48](#)
- [Advertising Routes into IPv6 Multiprotocol BGP, page 50](#)
- [Redistributing Prefixes into IPv6 Multiprotocol BGP, page 51](#)

- [Assigning a BGP Administrative Distance, page 52](#)
- [Generating Translate Updates for IPv6 Multicast BGP, page 53](#)
- [Resetting IPv6 BGP Sessions, page 54](#)
- [Clearing External BGP Peers, page 55](#)
- [Clearing IPv6 BGP Route Dampening Information, page 56](#)
- [Clearing IPv6 BGP Flap Statistics, page 56](#)

## Configuring an IPv6 Peer Group to Perform Multicast BGP Routing

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family ipv6** [**unicast** | **multicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>router bgp</b> <i>as-number</i>  <b>Example:</b> Device(config)# router bgp 65000	Enters router configuration mode for the specified BGP routing process.

Command or Action	Purpose
<p><b>Step 4</b> <code>neighbor peer-group-name peer-group</code></p> <p><b>Example:</b></p> <pre>Device(config-router)# neighbor group1 peer-group</pre>	<p>Creates a BGP peer group.</p>
<p><b>Step 5</b> <code>neighbor {ip-address   ipv6-address   peer-group-name} remote-as as-number</code></p> <p><b>Example:</b></p> <pre>Device(config-router)# neighbor 2001:DB8:0:CC00::1 remote-as 64600</pre>	<p>Adds the IPv6 address of the neighbor in the specified autonomous system to the IPv6 multicast BGP neighbor table of the local router.</p> <ul style="list-style-type: none"> <li>The <i>ipv6-address</i> argument in the <b>neighbor remote-as</b> command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> </ul>
<p><b>Step 6</b> <code>address-family ipv6 [unicast   multicast]</code></p> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv6 multicast</pre>	<p>Specifies the IPv6 address family, and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv6 unicast address family. By default, the router is placed in configuration mode for the IPv6 unicast address family if a keyword is not specified in the <b>address-family ipv6</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv6 multicast address prefixes.</li> </ul>
<p><b>Step 7</b> <code>neighbor {ip-address   peer-group-name   ipv6-address} activate</code></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 activate</pre>	<p>Enables the neighbor to exchange prefixes for the specified family type with the neighbor and the local router.</p> <ul style="list-style-type: none"> <li>To avoid extra configuration steps for each neighbor, use the <b>neighbor activate</b> command with the <i>peer-group-name</i> argument as an alternative in this step.</li> </ul>
<p><b>Step 8</b> <code>neighbor {ip-address   ipv6-address} peer-group peer-group-name</code></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 peer-group group1</pre>	<p>Assigns the IPv6 address of a BGP neighbor to a peer group.</p>

- [What to Do Next, page 49](#)

## What to Do Next

Refer to "Configuring an IPv6 Multiprotocol BGP Peer Group" in the Implementing Multiprotocol BGP for IPv6 document and the Cisco IOS IP Routing Configuration Guide for more information on assigning options to peer groups and making a BGP or multicast BGP neighbor a member of a peer group.

## Advertising Routes into IPv6 Multiprotocol BGP

Perform this task to advertise (inject) a prefix into IPv6 multicast BGP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **network** *ipv6-address / prefix-length*

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b>  <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b>  <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <b>router bgp</b> <i>as-number</i>  <b>Example:</b>  <pre>Router(config)# router bgp 65000</pre>	Enters router configuration mode for the specified BGP routing process.
<b>Step 4</b> <b>address-family ipv6</b> [ <b>unicast</b>   <b>multicast</b> ]  <b>Example:</b>  <pre>Router(config-router)# address-family ipv6 multicast</pre>	Specifies the IPv6 address family, and enters address family configuration mode. <ul style="list-style-type: none"> <li>• The <b>unicast</b> keyword specifies the IPv6 unicast address family. By default, the router is placed in configuration mode for the IPv6 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv6</b> command.</li> <li>• The <b>multicast</b> keyword specifies IPv6 multicast address prefixes.</li> </ul>

Command or Action	Purpose
<p><b>Step 5</b> <code>network ipv6-address / prefix-length</code></p> <p><b>Example:</b></p> <pre>Router(config-router-af)# network 2001:DB8::/24</pre>	<p>Advertises (injects) the specified prefix into the IPv6 BGP database. (The routes must first be found in the IPv6 unicast routing table.)</p> <ul style="list-style-type: none"> <li>Specifically, the prefix is injected into the database for the address family specified in the previous step.</li> <li>Routes are tagged from the specified prefix as "local origin."</li> <li>The <i>ipv6-prefix</i> argument in the <b>network</b> command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>The <i>prefix-length</i> argument is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</li> </ul>

## Redistributing Prefixes into IPv6 Multiprotocol BGP

Redistribution is the process of redistributing, or injecting, prefixes from one routing protocol into another routing protocol. This task explains how to inject prefixes from a routing protocol into IPv6 multiprotocol BGP. Specifically, prefixes that are redistributed into IPv6 multiprotocol BGP using the **redistribute** router configuration command are injected into the IPv6 unicast database.

### SUMMARY STEPS

- enable
- configure terminal
- router bgp *as-number*
- address-family ipv6 [*vrf vrf-name*] [**unicast** | **multicast** | **vpnv6**]
- redistribute bgp [*process-id*] [**metric** *metric-value*] [**route-map** *map-name*] [*source-protocol-options*]
- exit

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>

Command or Action	Purpose
<b>Step 3</b> <code>router bgp <i>as-number</i></code>  <b>Example:</b> <pre>Device(config)# router bgp 65000</pre>	Enters router configuration mode for the specified BGP routing process.
<b>Step 4</b> <code>address-family ipv6 [<i>vrf vrf-name</i>] [<b>unicast</b>   <b>multicast</b>   <b>vpnv6</b>]</code>  <b>Example:</b> <pre>Device(config-router)# address-family ipv6</pre>	Specifies the IPv6 address family, and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv6 unicast address family. By default, the router is placed in configuration mode for the IPv6 unicast address family if a keyword is not specified with the <b>address-family ipv6</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv6 multicast address prefixes.</li> </ul>
<b>Step 5</b> <code>redistribute bgp [<i>process-id</i>] [<b>metric</b> <i>metric-value</i>] [<b>route-map</b> <i>map-name</i>] [<i>source-protocol-options</i>]</code>  <b>Example:</b> <pre>Device(config-router-af)# redistribute bgp 64500 metric 5 metric-type external</pre>	Redistributes IPv6 routes from one routing domain into another routing domain.
<b>Step 6</b> <code>exit</code>  <b>Example:</b> <pre>Device(config-router-af)# exit</pre>	Exits address family configuration mode, and returns the router to router configuration mode. <ul style="list-style-type: none"> <li>Repeat this step to exit router configuration mode and return the router to global configuration mode.</li> </ul>

## Assigning a BGP Administrative Distance



### Caution

Changing the administrative distance of BGP internal routes is not recommended. One problem that can occur is the accumulation of routing table inconsistencies, which can break routing.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router bgp as-number`
4. `address-family ipv6 [unicast | multicast]`
5. `distance bgp external-distance internal-distance local-distance`

## DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>router bgp <i>as-number</i></code>  <b>Example:</b> <pre>Device(config)# router bgp 100</pre>	Enters router configuration mode for the specified routing process.
<b>Step 4</b> <code>address-family ipv6 [unicast   multicast]</code>  <b>Example:</b> <pre>Device(config-router)# address-family ipv6 multicast</pre>	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
<b>Step 5</b> <code>distance bgp <i>external-distance internal-distance local-distance</i></code>  <b>Example:</b> <pre>Device(config-router)# distance bgp 20 20 200</pre>	Assigns a BGP administrative distance.

## Generating Translate Updates for IPv6 Multicast BGP

The multicast BGP translate-update feature generally is used in a multicast BGP-capable router that peers with a customer site that has only a BGP-capable router; the customer site has not or cannot upgrade its router to a multicast BGP-capable image. Because the customer site cannot originate multicast BGP advertisements, the router with which it peers will translate the BGP prefixes into multicast BGP prefixes, which are used for multicast-source RPF lookup.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b>  Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b>  Device# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>router bgp</b> <i>as-number</i>  <b>Example:</b>  Device(config)# router bgp 100	Enters router configuration mode for the specified routing process.
<b>Step 4</b> <b>address-family ipv6</b> [ <b>unicast</b>   <b>multicast</b> ]  <b>Example:</b>  Device(config-router)# address-family ipv6 multicast	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
<b>Step 5</b> <b>neighbor</b> <i>ipv6-address</i> <b>translate-update ipv6 multicast</b> [ <b>unicast</b> ]  <b>Example:</b>  Device(config-router)# neighbor 2001:DB8:7000::2 translate-update ipv6 multicast	Generates multiprotocol IPv6 BGP updates that correspond to unicast IPv6 updates received from a peer.

**Resetting IPv6 BGP Sessions**

**SUMMARY STEPS**

1. enable
2. **clear bgp ipv6** {unicast | multicast} { \* | *autonomous-system-number* | *ip-address* | *ipv6-address* | **peer-group** *peer-group-name* } [soft] [in | out]

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> enable  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>clear bgp ipv6</b> {unicast   multicast} { *   <i>autonomous-system-number</i>   <i>ip-address</i>   <i>ipv6-address</i>   <b>peer-group</b> <i>peer-group-name</i> } [soft] [in   out]  <b>Example:</b> Device# clear bgp ipv6 unicast peer-group marketing soft out	Resets IPv6 BGP sessions.

**Clearing External BGP Peers****SUMMARY STEPS**

1. enable
2. **clear bgp ipv6** {unicast | multicast} external [soft] [in | out]
3. **clear bgp ipv6** {unicast | multicast} **peer-group** *name*

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> enable  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>clear bgp ipv6</b> {unicast   multicast} external [soft] [in   out]  <b>Example:</b> Device# clear bgp ipv6 unicast external soft in	Clears external IPv6 BGP peers.

	Command or Action	Purpose
<b>Step 3</b>	<code>clear bgp ipv6 {unicast   multicast} peer-group name</code>  <b>Example:</b>  Device# <code>clear bgp ipv6 unicast peer-group marketing</code>	Clears all members of an IPv6 BGP peer group.

## Clearing IPv6 BGP Route Dampening Information

### SUMMARY STEPS

1. `enable`
2. `clear bgp ipv6 {unicast | multicast} dampening [ipv6-prefix prefix-length]`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<code>enable</code>  <b>Example:</b>  Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<code>clear bgp ipv6 {unicast   multicast} dampening [ipv6-prefix prefix-length]</code>  <b>Example:</b>  Device# <code>clear bgp ipv6 unicast dampening 2001:DB8::/64</code>	Clears IPv6 BGP route dampening information and unsuppresses the suppressed routes.

## Clearing IPv6 BGP Flap Statistics

### SUMMARY STEPS

1. `enable`
2. `clear bgp ipv6 {unicast | multicast} flap-statistics [ipv6-prefix/prefix-length | regexp regexp | filter-list list]`

## DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>clear bgp ipv6 {unicast   multicast} flap-statistics [ipv6-prefix/prefix-length   regexp regexp   filter-list list]</code>  <b>Example:</b> <pre>Device# clear bgp ipv6 unicast flap-statistics filter-list 3</pre>	Clears IPv6 BGP flap statistics.

## Configuring Bandwidth-Based CAC for IPv6

- [Configuring the Interface Limit for Bandwidth-Based CAC in IPv6, page 57](#)
- [Configuring an Access List for Bandwidth-Based CAC in IPv6, page 58](#)
- [Configuring the Global Limit for Bandwidth-Based CAC in IPv6, page 60](#)

### Configuring the Interface Limit for Bandwidth-Based CAC in IPv6

Bandwidth-based CAC for IPv6 counts per-interface IPv6 mroute states using cost multipliers. With this feature, router administrators can specify which cost multiplier to use when accounting such state against the interface limits.

#### SUMMARY STEPS

- `enable`
- `configure terminal`
- `interface type number`
- `ipv6 address {ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}`
- `ipv6 multicast limit [connected | rpf | out] limit-acl max`

## DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>

Command or Action	Purpose
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>interface type number</code>  <b>Example:</b> <pre>Router(config)# interface FastEthernet 1/3</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 4</b> <code>ipv6 address {ipv6-address / prefix-length   prefix-name sub-bits / prefix-length}</code>  <b>Example:</b> <pre>Router(config-if)# ipv6 address FE80::40:1:3 link-local</pre>	Configures an IPv6 address based on an IPv6 general prefix.
<b>Step 5</b> <code>ipv6 multicast limit [connected   rpf   out] limit-acl max</code>  <b>Example:</b> <pre>Router (config-if)# ipv6 multicast limit out acl1 10</pre>	Configures per-interface mroute state limiters in IPv6.

## Configuring an Access List for Bandwidth-Based CAC in IPv6

In bandwidth-based CAC for IPv6, router administrators can configure global limit cost commands for state matching access lists. Perform this task to configure an access list to configure a state matching access list.

or

**deny**

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit**

## DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <code>ipv6 access-list <i>access-list-name</i></code></p> <p><b>Example:</b></p> <pre>Router(config)# ipv6 access-list costlist1</pre>	<p>Defines an IPv6 access list and places the router in IPv6 access list configuration mode.</p>
<p><b>Step 4</b> <code>permit</code></p> <p><b>Example:</b></p> <p><b>Example:</b></p> <p>or</p> <p><b>Example:</b></p> <p><b>Example:</b></p> <p style="text-align: center;"><b>deny</b></p> <p><b>Example:</b></p> <pre>Router(config-ipv6-acl)# permit any ff03::1/64</pre>	<p>Use the <b>permit</b> or <b>deny</b> command to set conditions for an IPv6 access list.</p>

## Configuring the Global Limit for Bandwidth-Based CAC in IPv6

Router administrators can configure global limit cost commands for state matching access lists.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast [vrf vrf-name] limit cost access-list cost-multiplier**

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1 enable</b>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2 configure terminal</b>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3 ipv6 multicast [vrf vrf-name] limit cost access-list cost-multiplier</b>  <b>Example:</b> <pre>Router (config)# ipv6 multicast limit cost costlist1 2</pre>	Applies a cost to mroutes that match per-interface mroute state limiters in IPv6.

## Using MFIB in IPv6 Multicast

Multicast forwarding is automatically enabled when IPv6 multicast routing is enabled.

- [Verifying MFIB Operation in IPv6 Multicast, page 60](#)
- [Resetting MFIB Traffic Counters, page 62](#)

### Verifying MFIB Operation in IPv6 Multicast

## SUMMARY STEPS

1. **enable**
2. **show ipv6 mfib** [*vrf vrf-name*] [**link-local** | **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name*] **active** | **count** | **interface** | **status** | **summary**]
3. **show ipv6 mfib** [*vrf vrf-name*] [**link-local** | *group-name* | *group-address*] **active** [*kbps*]
4. **show ipv6 mfib** [*vrf vrf-name*] [**all** | **linkscope** | *group-name* | *group-address* [*source-name* | *source-address*]] **count**
5. **show ipv6 mfib interface**
6. **show ipv6 mfib status**
7. **show ipv6 mfib** [*vrf vrf-name*] **summary**
8. **debug ipv6 mfib** [*vrf vrf-name*] [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**]

## DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <b>show ipv6 mfib</b> [<i>vrf vrf-name</i>] [<b>link-local</b>   <b>verbose</b>   <i>group-address-name</i>   <i>ipv6-prefix / prefix-length</i>   <i>source-address-name</i>] <b>active</b>   <b>count</b>   <b>interface</b>   <b>status</b>   <b>summary</b>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 mfib</pre>	<p>Displays the forwarding entries and interfaces in the IPv6 MFIB.</p>
<p><b>Step 3</b> <b>show ipv6 mfib</b> [<i>vrf vrf-name</i>] [<b>link-local</b>   <i>group-name</i>   <i>group-address</i>] <b>active</b> [<i>kbps</i>]</p> <p><b>Example:</b></p> <pre>Router# show ipv6 mfib active</pre>	<p>Displays the rate at which active sources are sending to multicast groups.</p>
<p><b>Step 4</b> <b>show ipv6 mfib</b> [<i>vrf vrf-name</i>] [<b>all</b>   <b>linkscope</b>   <i>group-name</i>   <i>group-address</i> [<i>source-name</i>   <i>source-address</i>]] <b>count</b></p> <p><b>Example:</b></p> <pre>Router# show ipv6 mfib count</pre>	<p>Displays summary traffic statistics from the MFIB about the group and source.</p>

Command or Action	Purpose
<p><b>Step 5</b> <code>show ipv6 mfib interface</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 mfib interface</pre>	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.
<p><b>Step 6</b> <code>show ipv6 mfib status</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 mfib status</pre>	Displays general MFIB configuration and operational status.
<p><b>Step 7</b> <code>show ipv6 mfib [vrf vrf-name] summary</code></p> <p><b>Example:</b></p> <pre>Router# show ipv6 mfib summary</pre>	Displays summary information about the number of IPv6 MFIB entries and interfaces.
<p><b>Step 8</b> <code>debug ipv6 mfib [vrf vrf-name] [group-name  group-address] [adjacency   db   fs   init   interface   mrib [detail]   nat   pak   platform   ppr   ps   signal   table]</code></p> <p><b>Example:</b></p> <pre>Router# debug ipv6 mfib FF04::10 pak</pre>	Enables debugging output on the IPv6 MFIB.

## Resetting MFIB Traffic Counters

### SUMMARY STEPS

1. `enable`
2. `clear ipv6 mfib [vrf vrf-name] counters [group-name | group-address [source-address | source-name]]`

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

Command or Action	Purpose
<p><b>Step 2</b> <code>clear ipv6 mfib [vrf vrf-name] counters [group-name   group-address [source-address   source-name]]</code></p> <p><b>Example:</b></p> <pre>Router# clear ipv6 mfib counters FF04::10</pre>	Resets all active MFIB traffic counters.

## Disabling Default Features in IPv6 Multicast

Several features are automatically enabled when IPv6 multicast is used. However, a user may want to disable certain features in response to certain situations.

- [Disabling Embedded RP Support in IPv6 PIM, page 63](#)
- [Turning Off IPv6 PIM on a Specified Interface, page 64](#)
- [Disabling MLD Router-Side Processing, page 65](#)
- [Disabling MFIB on the Router, page 66](#)
- [Disabling MFIB on a Distributed Platform, page 67](#)
- [Disabling MFIB Interrupt-Level IPv6 Multicast Forwarding, page 68](#)
- [Examples, page 68](#)

## Disabling Embedded RP Support in IPv6 PIM

A user might want to disable embedded RP support on an interface if all of the routers in the domain do not support embedded RP.



### Note

This task disables PIM completely, not just embedded RP support in IPv6 PIM.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `no ipv6 pim [vrf vrf-name] rp embedded`
4. `interface type number`
5. `no ipv6 pim`

## DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>no ipv6 pim [vrf vrf-name] rp embedded</code>  <b>Example:</b> <pre>Router(config)# no ipv6 pim rp embedded</pre>	Disables embedded RP support in IPv6 PIM.
<b>Step 4</b> <code>interface type number</code>  <b>Example:</b> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 5</b> <code>no ipv6 pim</code>  <b>Example:</b> <pre>Router(config-if)# no ipv6 pim</pre>	Turns off IPv6 PIM on a specified interface.

## Turning Off IPv6 PIM on a Specified Interface

A user might want only specified interfaces to perform IPv6 multicast and will therefore want to turn off PIM on a specified interface.

## SUMMARY STEPS

- `enable`
- `configure terminal`
- `interface type number`
- `no ipv6 pim`

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>interface type number</code>  <b>Example:</b> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 4</b> <code>no ipv6 pim</code>  <b>Example:</b> <pre>Router(config-if)# no ipv6 pim</pre>	Turns off IPv6 PIM on a specified interface.

**Disabling MLD Router-Side Processing**

A user might want only specified interfaces to perform IPv6 multicast and will therefore want to turn off MLD router-side processing on a specified interface.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `no ipv6 mld router`

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>interface type number</code>  <b>Example:</b> <pre>Router(config)# interface FastEthernet 1/0</pre>	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 4</b> <code>no ipv6 mld router</code>  <b>Example:</b> <pre>Router(config-if)# no ipv6 mld router</pre>	Disables MLD router-side processing on a specified interface.

**Disabling MFIB on the Router**

Multicast forwarding is automatically enabled when IPv6 multicast routing is enabled. However, a user may want to disable multicast forwarding on the router.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `no ipv6 mld router`

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>no ipv6 mfib</b>  <b>Example:</b> Router(config)# no ipv6 mfib	Disables IPv6 multicast forwarding on the router.

## Disabling MFIB on a Distributed Platform

Multicast forwarding is automatically enabled when IPv6 multicast routing is enabled. However, a user may want to disable multicast forwarding on a distributed platform.

### SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 mfib-mode centralized-only

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 mfib-mode centralized-only</b>  <b>Example:</b> Router(config)# ipv6 mfib-mode centralized-only	Disables distributed forwarding on a distributed platform.

## Disabling MFIB Interrupt-Level IPv6 Multicast Forwarding

MFIB interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface is enabled on interfaces that support Cisco Express Forwarding. However, you may want to disable MFIB interrupt-level forwarding on a specified interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 mfib cef output**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b>  Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b>  Router(config)# interface FastEthernet 1/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	<b>no ipv6 mfib cef output</b>  <b>Example:</b>  Router(config-if)# no ipv6 mfib cef output	Disables MFIB interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface.

### Examples

This section provides the following command output examples:

### Sample Output from the show ipv6 mfib Command

The following example displays the forwarding entries and interfaces in the MFIB. The router is configured for fast switching, and it has a receiver joined to FF05::1 on Ethernet1/1 and a source (2001:DB8:1:1:20) sending on Ethernet1/2:

```
Router# show ipv6 mfib
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
(*,FF00::/8) Flags: C
  Forwarding: 0/0/0/0, Other: 0/0/0
  Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
  Forwarding: 2/0/100/0, Other: 0/0/0
  Tunnel0 Flags: A NS
  Ethernet1/1 Flags: F NS
    Pkts: 0/2
(2001:DB8:1:1:200,FF05::1) Flags:
  Forwarding: 5/0/100/0, Other: 0/0/0
  Ethernet1/2 Flags: A
  Ethernet1/1 Flags: F NS
    Pkts: 3/2
(*,FF10::/15) Flags: D
  Forwarding: 0/0/0/0, Other: 0/0/0
```

### Sample Output from the show ipv6 mfib active Command

The following example displays statistics on the rate at which active IP multicast sources are sending information. The router is switching traffic from 2001:DB8:1:1:200 to FF05::1:

```
Router# show ipv6 mfib active
Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001:DB8:1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

### Sample Output from the show ipv6 mfib count Command

The following example displays statistics from the MFIB about the group and source. The router is switching traffic from 2001:DB8:1:1:200 to FF05::1:

```
Router# show ipv6 mfib count
IP Multicast Statistics
54 routes, 7 groups, 0.14 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: FF00::/8
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF00::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF05::1
  RP-tree: Forwarding: 2/0/100/0, Other: 0/0/0
  Source: 10::1:1:200, Forwarding: 367/10/100/7, Other: 0/0/0
  Tot. shown: Source count: 1, pkt count: 369
Group: FF10::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF20::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
```

### Sample Output from the show ipv6 mfib interface Command

The following example displays information about IPv6 multicast-enabled interfaces and their forwarding status. The router is configured for fast switching:

```
Router# show ipv6 mfib interface
IPv6 Multicast Forwarding (MFIB) status:
  Configuration Status: enabled
  Operational Status: running
MFIB interface      status      CEF-based output
                   [configured,available]
Ethernet1/1         up          [yes        ,yes    ]
Ethernet1/2         up          [yes        ,?      ]
Tunnel0             up          [yes        ,?      ]
Tunnell            up          [yes        ,?      ]
```

### Sample Output from the show ipv6 mfib summary Command

The following example displays summary information about the number of IPv6 MFIB entries and interfaces:

```
Router# show ipv6 mfib summary

IPv6 MFIB summary:
  54    total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17    total MFIB interfaces
```

### Sample Output from the show ipv6 mld groups Command

The following is sample output from the **show ipv6 mld groups** command. It shows all of the groups joined by Fast Ethernet interface 2/1, including link-local groups used by network protocols.

```
Router# show ipv6 mld groups FastEthernet 2/1
MLD Connected Group Membership
Group Address      Interface          Uptime      Expires
FF02::2            FastEthernet2/1   3d18h      never
FF02::D            FastEthernet2/1   3d18h      never
FF02::16           FastEthernet2/1   3d18h      never
FF02::1:FF00:1     FastEthernet2/1   3d18h      00:00:27
FF02::1:FF00:79    FastEthernet2/1   3d18h      never
FF02::1:FF23:83C2  FastEthernet2/1   3d18h      00:00:22
FF02::1:FFAF:2C39  FastEthernet2/1   3d18h      never
FF06:7777::1      FastEthernet2/1   3d18h      00:00:26
```

### Sample Output from the show ipv6 mld groups summary Command

The following is sample output from the **show ipv6 mld groups summary** command:

```
Router# show ipv6 mld groups summary
MLD Route Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 0
```

### Sample Output from the show ipv6 mld interface Command

The following is sample output from the **show ipv6 mld interface** command for Fast Ethernet interface 2/1:

```
Router# show ipv6 mld interface FastEthernet 2/1
FastEthernet2/1 is up, line protocol is up
Internet address is FE80::205:5FFF:FEAF:2C39/10
MLD is enabled in 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: 25 joins, 17 leaves
MLD querying router is FE80::205:5FFF:FEAF:2C39 (this system)

```

### Sample Output from the show ipv6 mld ssm-map Command

The following examples show SSM mapping for the source address 2001:DB8::1:

```

Router# show ipv6 mld ssm-map 2001:DB8::1
  Group address : 2001:DB8::1
  Group mode ssm : TRUE
  Database      : STATIC
  Source list   : 2001:DB8::2
                 2001:DB8::3
Router# show ipv6 mld ssm-map 2001:DB8::2
  Group address : 2001:DB8::2
  Group mode ssm : TRUE
  Database      : DNS
  Source list   : 2001:DB8::3
                 2001:DB8::1

```

### Sample Output from the show ipv6 mld traffic Command

The following example displays the MLD protocol messages received and sent:

```

Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

```

	Received	Sent
Valid MLD Packets	3	1
Queries	1	0
Reports	2	1
Leaves	0	0
Mtrace packets	0	0
Errors:		
Malformed Packets		0
Bad Checksums		0
Martian source		0
Packets Received on MLD-disabled Interface		0

### Sample Output from the show ipv6 mrrib client Command

The following is sample output from the `show ipv6 mrrib client` command:

```

Router# show ipv6 mrrib client
IP MRIB client-connections
igmp:145      (connection id 0)
pim:146      (connection id 1)
mfib ipv6:3   (connection id 2)
slot 3 mfib ipv6 rp agent:16 (connection id 3)
slot 1 mfib ipv6 rp agent:16 (connection id 4)
slot 0 mfib ipv6 rp agent:16 (connection id 5)
slot 4 mfib ipv6 rp agent:16 (connection id 6)
slot 2 mfib ipv6 rp agent:16 (connection id 7)

```

### Sample Output from the show ipv6 mrrib route Command

The following is sample output from the `show ipv6 mrrib route` command using the `summary` keyword:

```

Router# show ipv6 mrrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10

```

### Sample Output from the show ipv6 mroute Command

Using the **show ipv6 mroute** command is a good way to dynamically verify that multicast IPv6 data is flowing. The following is sample output from the **show ipv6 mroute** command:

```
Router# show ipv6 mroute ff07::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
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:45/00:02:47, RP 2001:DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6:6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47
(2001:DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

### Sample Output from the show ipv6 mroute active Command

The following is sample output from the **show ipv6 mroute active** command:

```
Router# show ipv6 mroute active
Active IPv6 Multicast Sources - sending >= 4 kbps
Group:FF05::1
  Source:2001:DB8:1:1:1
    Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

### Sample Output from the show ipv6 pim bsr Command

The following example displays BSR election information:

```
Router# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 2001:DB8:1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 2001:DB8:1:1:4, priority: 0, hash mask length: 126
```

### Sample Output from the show ipv6 pim group-map Command

The following is sample output from the **show ipv6 pim group-map** command:

```
Router# show ipv6 pim group-map
FF33::/32*
  SSM
  Info source:Static
  Uptime:00:08:32, Groups:0
FF34::/32*
  SSM
  Info source:Static
  Uptime:00:09:42, Groups:0
```

### Sample Output from the show ipv6 pim interface Command

The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword:

```
Router# show ipv6 pim interface state-on
Interface          PIM  Nbr  Hello  DR
                   Count Intvl Prior
Ethernet0          on   0    30    1
  Address:FE80::208:20FF:FE08:D7FF
  DR      :this system
POS1/0             on   0    30    1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
POS4/0             on   1    30    1
  Address:FE80::208:20FF:FE08:D554
  DR      :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0    30    1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
Loopback0          on   0    30    1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
```

### Sample Output from the show ipv6 pim join-prune statistic Command

The following example provides the join/prune aggregation on Ethernet interface 0/0/0:

```
Router# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted          Received
Ethernet0/0/0      0 / 0 / 0           1 / 0 / 0
```

### Sample Output from the show ipv6 pim neighbor Command

The following is sample output from the **show ipv6 pim neighbor** command using the **detail** keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
Router# show ipv6 pim neighbor detail
Neighbor Address(es)      Interface          Uptime    Expires DR pri Bidir
FE80::A8BB:CCFF:FE00:401  Ethernet0/0       01:34:16  00:01:16 1    B
60::1:1:3
FE80::A8BB:CCFF:FE00:501  Ethernet0/0       01:34:15  00:01:18 1    B
60::1:1:4
```

### Sample Output from the show ipv6 pim range-list Command

The following is sample output from the **show ipv6 pim range-list** command:

```
Router# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
FF33::/32 Up:00:26:33
FF34::/32 Up:00:26:33
FF35::/32 Up:00:26:33
FF36::/32 Up:00:26:33
FF37::/32 Up:00:26:33
FF38::/32 Up:00:26:33
FF39::/32 Up:00:26:33
FF3A::/32 Up:00:26:33
FF3B::/32 Up:00:26:33
FF3C::/32 Up:00:26:33
FF3D::/32 Up:00:26:33
FF3E::/32 Up:00:26:33
FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
FF09::/64 Up:00:03:50
```

### Sample Output from the show ipv6 pim topology Command

The following is sample output from the **show ipv6 pim topology** command:

```
Router# show ipv6 pim topology
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
(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:2001:DB8:1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1      02:26:56  fwd LI LH
(2001:DB8:1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1      00:00:07  off LI
```

### Sample Output from the show ipv6 pim traffic Command

The following example shows the number of PIM protocol messages received and sent.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

```

	Received	Sent
Valid PIM Packets	22	22
Hello	22	22
Join-Prune	0	0
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

### Sample Output from the show ipv6 pim tunnel Command

The following is sample output from the **show ipv6 pim tunnel** command on the RP:

```
Router# show ipv6 pim tunnel
Tunnel0*
  Type :PIM Encap
  RP   :100::1
  Source:100::1
Tunnel0*
  Type :PIM Decap
  RP   :100::1
  Source: -
```

The following is sample output from the **show ipv6 pim tunnel** command on a non-RP:

```
Router# show ipv6 pim tunnel
Tunnel0*
  Type :PIM Encap
```

```
RP      :100::1
Source:2001::1:1:1
```

### Sample Output from the show ipv6 rpf Command

The following example displays RPF information for the unicast host with the IPv6 address of 2001:DB8:1:1:2:

```
Router# show ipv6 rpf 2001:DB8:1:1:2
RPF information for 2001:DB8:1:1:2
RPF interface:Ethernet3/2
RPF neighbor:FE80::40:1:3
RPF route/mask:20::/64
RPF type:Unicast
RPF recursion count:0
Metric preference:110
Metric:30
```

## Configuration Examples for Implementing IPv6 Multicast

- [Example: Enabling IPv6 Multicast Routing, page 75](#)
- [Example: Configuring the MLD Protocol, page 75](#)
- [Example: Configuring Explicit Tracking of Receivers, page 76](#)
- [Example: Configuring MLD Proxy, page 77](#)
- [Example: Configuring PIM, page 77](#)
- [Example: Configuring PIM Options, page 77](#)
- [Example Configuring Mroutes, page 78](#)
- [Example Configuring an IPv6 Multiprotocol BGP Peer Group, page 78](#)
- [Example Redistributing Prefixes into IPv6 Multiprotocol BGP, page 78](#)
- [Example: Generating Translate Updates for IPv6 Multicast BGP, page 78](#)
- [Example: Configuring Bandwidth-Based CAC for IPv6, page 78](#)
- [Example: Disabling Embedded RP Support in IPv6 PIM, page 79](#)
- [Example Turning Off IPv6 PIM on a Specified Interface, page 79](#)
- [Example: Disabling MLD Router-Side Processing, page 79](#)
- [Example Disabling and Reenabling MFIB, page 79](#)

### Example: Enabling IPv6 Multicast Routing

The following example enables multicast routing on all interfaces. Entering this command also enables multicast forwarding for PIM and MLD on all enabled interfaces of the router.

```
Router> enable
Router# configure terminal

Router(config)# ipv6 multicast-routing
```

### Example: Configuring the MLD Protocol

The following example shows how to configure the query maximum response time, the query timeout, and the query interval on FastEthernet interface 1/0:

```
Router> enable
```

```

Router# configure terminal
Router(config)# interface FastEthernet 1/0

Router(config-if)# ipv6 mld query-max-response-time 20

Router(config-if)# ipv6 mld query-timeout 130

Router(config-if)# ipv6 mld query-interval 60

```

The following example shows how to configure MLD reporting for a specified group and source, allows the user to perform IPv6 multicast receiver access control, and statically forwards traffic for the multicast group onto FastEthernet interface 1/0:

```

Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 1/0
Router(config)# ipv6 mld join-group FF04::10
Router(config)# ipv6 mld static-group FF04::10 100::1
Router(config)# ipv6 mld access-group acc-grp-1

```

The following example shows information from the **show ipv6 mld interface** command for Fast Ethernet interface 2/1:

```

Router# show ipv6 mld interface FastEthernet 2/1

FastEthernet2/1 is up, line protocol is up
Internet address is FE80::205:5FFF:FEAF:2C39/10
MLD is enabled in 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: 25 joins, 17 leaves
MLD querying router is FE80::205:5FFF:FEAF:2C39 (this system)

```

The following example displays the MLD protocol messages received and sent:

```

Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

          Received      Sent
Valid MLD Packets          3          1
Queries                    1          0
Reports                    2          1
Leaves                     0          0
Mtrace packets             0          0

Errors:
Malformed Packets                0
Bad Checksums                    0
Martian source                   0
Packets Received on MLD-disabled Interface 0

```

## Example: Configuring Explicit Tracking of Receivers

```

Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld explicit-tracking list1

```

## Example: Configuring MLD Proxy

The following example shows how to configure IPv6 MLD proxy information for the Ethernet 0/0 interface and information about the configured interface:

```
Router(config)# ipv6 mld host-proxy Ethernet0/0
Router(config)# exit
Router# show ipv6 mld host-proxy Ethernet0/0
Ethernet0/0 is up, line protocol is up
  Internet address is FE80::34/64
MLD is enabled on interface
  MLD querying router is FE80::12, Version: MLDv2
  Current MLD host version is 2
  MLD max query response time is 10 seconds
Number of MLD Query sent on interface : 10
Number of MLD Query received on interface : 20
Number of MLDv1 report sent : 5
Number of MLDv2 report sent : 10
Number of MLDv1 leave sent : 0
Number of MLDv2 leave sent : 1
```

The following example configure a group entry for the Ethernet 0/0 proxy interface and provides information about those group entries:

```
Router# show ipv6 mld host-proxy Ethernet0/0 group
Group:                FF5E::12
Uptime:               00:00:07
Group mode:           INCLUDE
Version               MLDv2
Group source list:
  Source Address      Uptime
  5000::2             00:00:07
  2000::2             00:01:15
Group:                FF7E::21
Uptime:               00:02:07
Group mode:           EXCLUDE
Version               MLDv2
Group source list: Empty
```

## Example: Configuring PIM

The following example shows how to configure a router to use PIM-SM using 2001:DB8::1 as the RP. It sets the SPT threshold to infinity to prevent switchover to the source tree when a source starts sending traffic and sets a filter on all sources that do not have a local multicast BGP prefix.

```
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 pim rp-address 2001:DB8::1
Router(config)# ipv6 pim spt-threshold infinity
Router(config)# ipv6 pim accept-register route-map reg-filter
```

## Example: Configuring PIM Options

The following example sets the DR priority, the PIM hello interval, and the periodic join and prune announcement interval on Ethernet interface 0/0.

```
Router(config)# interface Ethernet0/0
Router(config)# ipv6 pim hello-interval 60
Router(config)# ipv6 pim dr-priority 3
```

## Example Configuring Mroutes

The following example shows how to configure a static multicast route to be used for multicast RPF selection only:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 route 2001:DB8::/64 7::7 100 multicast
```

## Example Configuring an IPv6 Multiprotocol BGP Peer Group

The following example configures the IPv6 multiprotocol BGP peer group named group1:

```
router bgp 65000
no bgp default ipv4-unicast
neighbor group1 peer-group
neighbor 2001:DB8:0:CC00::1 remote-as 64600
address-family ipv6 multicast
neighbor 3FFE:C00:0:1:A8BB:CCFF:FE00:8200 activate
no auto-summary
no synchronization
exit-address-family
```

## Example Redistributing Prefixes into IPv6 Multiprotocol BGP

The following example redistributes BGP routes into the IPv6 multicast database of the local router:

```
router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 multicast
redistribute BGP
```

## Example: Generating Translate Updates for IPv6 Multicast BGP

The following example shows how to generate IPv6 multicast BGP updates that correspond to unicast IPv6 updates:

```
router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 multicast
neighbor 2001:DB8:7000::2 translate-update ipv6 multicast
```

## Example: Configuring Bandwidth-Based CAC for IPv6

- [Example: Configuring the Interface Limit for Bandwidth-Based CAC in IPv6, page 78](#)
- [Example: Configuring an Access List for Bandwidth-Based CAC in IPv6, page 79](#)
- [Example: Configuring the Global Limit for Bandwidth-Based CAC, page 79](#)

## Example: Configuring the Interface Limit for Bandwidth-Based CAC in IPv6

The following example configures the interface limit on the source router's outgoing interface Ethernet 1/3.

```
interface Ethernet1/3
ipv6 address FE80::40:1:3 link-local
```

```
ipv6 address 2001:DB8:1:1:3/64
ipv6 multicast limit out acl1 10
```

## Example: Configuring an Access List for Bandwidth-Based CAC in IPv6

The following example shows how to configure an access list to use for bandwidth-based CAC:

```
ipv6 access-list cost-list
 permit any ff03::1/64
```

## Example: Configuring the Global Limit for Bandwidth-Based CAC

The following example configures the global limit on the source router.

```
ipv6 multicast limit cost cost-list 2
```

## Example: Disabling Embedded RP Support in IPv6 PIM

The following example disables embedded RP support on IPv6 PIM:

```
Router(config)# ipv6 multicast-routing
Router(config)# no ipv6 pim rp embedded
```

## Example Turning Off IPv6 PIM on a Specified Interface

The following example turns off IPv6 PIM on FastEthernet interface 1/0:

```
Router(config)# ipv6 multicast-routing
Router(config)# interface FastEthernet 1/0
Router(config)# no ipv6 pim
```

## Example: Disabling MLD Router-Side Processing

The following example turns off MLD router-side processing on GigabitEthernet interface 1/0/0:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 1/0/0

Router(config-if)# no ipv6 mld router
```

## Example Disabling and Reenabling MFIB

Multicast forwarding is automatically enabled when IPv6 multicast routing is enabled; however, a user may want to disable multicast forwarding on the router. The following example shows how to disable multicast forwarding on the router and, if desired, reenables multicast forwarding on the router. The example also shows how to disable MFIB interrupt-level IPv6 multicast forwarding of outgoing packets on FastEthernet interface 1/0:

```
Router> enable
Router# configure terminal
Router(config) no ipv6 mfib
Router(config) ipv6 mfib-mode centralized-only
Router(config) interface FastEthernet 1/0
Router(config-if) no ipv6 mfib cef output
```

# Additional References

## Related Documents

Related Topic	Document Title
IPv6 multicast addresses	"Implementing IPv6 Addressing and Basic Connectivity," <i>Cisco IOS IPv6 Configuration Guide</i>
Multicast BGP for IPv6	"Implementing Multiprotocol BGP for IPv6," <i>Cisco IOS IPv6 Configuration Guide</i>
IPv6 static routes	"Implementing Static Routes for IPv6," <i>Cisco IOS IPv6 Configuration Guide</i>
IPv6 tunnels	"Implementing Tunneling for IPv6," <i>Cisco IOS IPv6 Configuration Guide</i>

## Standards

Title
<i>Protocol Independent Multicast - Sparse Mode PIM-SM): Protocol Specification (Revised)</i> , March 6, 2003
<i>Embedding the Address of RP in IPv6 Multicast Address</i> , May 23, 2003
<i>PIM Upstream Detection Among Multiple Addresses</i> , February 2003
<i>Bi-directional Protocol Independent Multicast (BIDIR-PIM)</i> , June 20, 2003
<i>Bootstrap Router (BSR) Mechanism for PIM Sparse Mode</i> , February 25, 2003

## MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2373	<i>IP Version 6 Addressing Architecture</i>

<b>RFC</b>	<b>Title</b>
RFC 2375	<i>IPv6 Multicast Address Assignments</i>
RFC 2460	<i>Internet Protocol, Version 6 (IPv6) Specification</i>
RFC 2461	<i>Neighbor Discovery for IP version 6 (IPv6)</i>
RFC 2462	<i>IPv6 Stateless Address Autoconfiguration</i>
RFC 2710	<i>Multicast Listener Discovery (MLD) for IPv6</i>
RFC 2711	<i>IPv6 Router Alert Option</i>
RFC 3576	<i>Change of Authorization</i>
RFC 3590	<i>Source Address Selection for the Multicast Listener Discovery (MLD) Protocol</i>
RFC 3810	<i>Multicast Listener Discovery Version 2 (MLDv2) for IPv6</i>
RFC 3956	<i>Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address</i>
RFC 4007	<i>IPv6 Scoped Address Architecture</i>

#### Technical Assistance

<b>Description</b>	<b>Link</b>
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Implementing IPv6 Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1** *Feature Information for Implementing IPv6 Multicast*

<b>Feature Name</b>	<b>Releases</b>	<b>Feature Information</b>
IPv6 Multicast	12.0(26)S 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.3(2)T	IPv6 multicast allows a host to send a single data stream to a subset of all hosts simultaneously.
IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 15.0(1)S	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, and 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.
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 15.0(1)S	PIM-SM uses unicast routing to provide reverse-path information for multicast tree building. PIM-SM is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic.
IPv6 Multicast: PIM Source Specific Multicast (PIM-SSM)	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 15.0(1)S 15.0(1)SG	PIM-SSM supports the implementation of SSM and is derived from PIM-SM. The SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, optimizing bandwidth utilization and denying unwanted Internet broadcast traffic.

Feature Name	Releases	Feature Information
IPv6 Multicast: Scope Boundaries	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 15.0(1)S	IPv6 includes support for global and nonglobal addresses. This section describes the usage of IPv6 addresses of different scopes.
IPv6 Multicast: MLD Access Group	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 15.0(1)S	The MLD access group provides receiver access control in Cisco IOS IPv6 multicast routers.
IPv6 Multicast: PIM Accept Register	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 15.0(1)S	The PIM accept register feature is the ability to perform PIM-SM register message filtering at the RP.
IPv6 Multicast: PIM Embedded RP Support	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 15.0(1)S	Embedded RP support allows the router to learn RP information using the multicast group destination address instead of the statically configured RP.
IPv6 Multicast: RPF Flooding of BSR Packets	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 15.0(1)S	The RPF flooding of BSR packets enables a Cisco IOS IPv6 router to not disrupt the flow of BSMs.

Feature Name	Releases	Feature Information
IPv6 Multicast: Routable Address Hello Option	12.0(26)S	The routable address hello option adds a PIM hello message option that includes all the addresses on the interface on which the PIM hello message is advertised.
	12.3(4)T	
	12.2(25)S	
	12.2(25)SG	
	12.2(33)SRA	
	12.2(33)SXH	
	15.0(1)S	
IPv6 Multicast: Static Multicast Routing (mroute)	12.0(26)S	IPv6 static mroutes share the same database as IPv6 static routes and are implemented by extending static route support.
	12.3(4)T	
	12.2(25)S	
	12.2(33)SRA	
	12.2(33)SXH	
	15.0(1)S	
IPv6 Multicast: Address Family Support for Multiprotocol BGP	12.0(26)S	This feature provides multicast BGP extensions for IPv6 and supports the same features and functionality as IPv4 BGP.
	12.2(25)S	
	12.2(25)SG	
	12.2(33)SRA	
	12.2(33)SXH	
	12.3(4)T	
	15.0(1)S	
IPv6 Multicast: Explicit Tracking of Receivers	12.2(25)S	This feature allows a router to track the behavior of the hosts within its IPv6 network.
	12.2(25)SG	
	12.2(33)SRA	
	12.2(33)SXH	
	12.3(7)T	
	15.0(1)S	
IPv6 Multicast: IPv6 Bidirectional PIM	12.2(25)SG	Bidirectional PIM allows multicast routers to keep reduced state information. Bidirectional shared trees convey data from sources to the RP and distribute them from the RP to the receivers.
	12.2(33)SRA	
	12.2(25)S	
	12.3(7)T	
	15.0(1)S	

Feature Name	Releases	Feature Information
IPv6 Multicast: MRIB	12.0(26)S 12.2(18)S 12.2(25)SG 12.3(2)T	The MRIB is a protocol-independent repository of multicast routing entries instantiated by multicast routing protocols (routing clients).
IPv6 Multicast: MFIB and MFIB Display Enhancements	12.0(26)S 12.2(18)S 12.3(2)T	The MFIB is a platform-independent and routing-protocol-independent library for IPv6 software.
IPv6 Multicast: Bootstrap Router (BSR)	12.0(28)S 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(11)T 15.0(1)S	If an RP becomes unreachable, this feature allows the RP to be detected and the mapping tables modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.
IPv6 Multicast: IPv6 BSR Bidirectional Support	12.2(33)SRE 12.3(14)T 15.0(1)S	Bidirectional BSR support allows bidirectional RPs to be advertised in C-RP messages and bidirectional ranges in the BSM.
IPv6 Multicast: IPv6 BSR Scoped-Zone Support	12.2(18)SXE	
IPv6 Multicast: SSM Mapping	12.2(33)SRA 12.2(18)SXE 12.4(2)T 15.0(1)S	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.
IPv6 Multicast: IPv6 BSR-Configure RP Mapping	12.2(33)SRE 12.2(50)SY 12.4(2)T 15.0(1)S 15.1(1)SG	This feature allows IPv6 multicast routers to be statically configured to announce scope-to-RP mappings directly from the BSR instead of learning them from candidate-RP messages.

Feature Name	Releases	Feature Information
IPv6 Multicast: MLD Group Limits	12.2(33)SRE	The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets.
	12.2(50)SY	
	12.4(2)T	
	15.0(1)S	
	15.1(1)SG	
IPv6 Multicast: Multicast User Authentication and ProfileSupport	12.4(4)T	Multicast access control provides an interface between multicast and AAA for provisioning, authorizing, and accounting at the last-hop router, receiver access control functions in multicast, and group or channel disabling capability in multicast.
IPv6 Multicast: Process Switching and Fast Switching	12.0(26)S	In IPv6 multicast process switching, the Route Processor must examine, rewrite, and forward each packet. IPv6 multicast fast switching allows routers to provide better packet forwarding performance than process switching.
	12.2(18)S	
	12.3(2)T	
Distributed MFIB (dMFIB)	12.0(26)S	Distributed MFIB dMFIB is used to switch multicast IPv6 packets on distributed platforms.
	12.2(25)S	
	12.3(4)T	
IPv6: Multicast Address Group Range Support	12.2(33)SRE	This feature allows the router to keep from receiving multicast traffic to be received from unauthenticated groups or unauthorized channels.
	12.2(33)SXI	
	15.0(1)M	
	15.0(1)S	
IPv6 Multicast: Bandwidth-Based Call Admission Control (CAC)	12.2(33)SRE	The bandwidth-based call admission control (CAC) for IPv6 multicast feature implements a method to monitor bandwidth per interface and multicast group avoiding oversubscription due to multicast services.
	15.0(1)S	
ISSU: IPv6 Multicast	15.0(1)SY	This feature is supported.
NSF/SSO: IPv6 Multicast	12.2(33)SRE	This feature is supported in Cisco IOS Release 12.2(33)SRE.
	15.0(1)SY	

Feature Name	Releases	Feature Information
MFIB: IPv4 SSO/ISSU	12.2(33)SRE	This feature is supported in Cisco IOS Release 12.2(33)SRE.
MLD Proxy	15.1(2)T	The MLD proxy feature enables a device to learn proxy group membership information, and forward multicast packets based upon that information.
IPv6 Multicast VRF Lite	15.1(4)M	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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.