



# IPv6 Multicast PIM

---

This module describes how to configure IPv6 Multicast PIM features.

- [Finding Feature Information, on page 1](#)
- [Prerequisites for IPv6 Multicast, on page 1](#)
- [Restrictions for IPv6 Multicast, on page 1](#)
- [Information About IPv6 Multicast, on page 2](#)
- [How to Configure IPv6 Multicast, on page 8](#)
- [Configuration Examples for IPv6 Multicast, on page 19](#)
- [Additional References, on page 23](#)
- [Feature Information for IPv6 Multicast PIM, on page 23](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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.

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 IPv6 Multicast

The following are the prerequisites for IPv6 PIM source-specific multicast (SSM):

- Multicast Listener Discovery (MLD) version 2 is required for source-specific multicast (SSM) to operate.
- Before configuring SSM with MLD, SSM must be supported by the Cisco IPv6 device, the host where the application is running, and the application itself.

## Restrictions for IPv6 Multicast

The supported IPv6 scale for the default templates for multicast routes is 500.

The router does *not* support :

- IPv6 Multicast Listener Discovery (MLD) snooping
- Bootstrap Router (BSR)
- Multiprotocol BGP Extensions for multicast
- Equal Cost Multipath (ECMP) for multicast
- Multicast Virtual Private Network (MVPN)
- Multicast QoS
- Dynamic Domain Name System (DNS) PIM Source Specific Multicast (SSM) mapping for multicast
- Multicast Source Discovery Protocol (MSDP)



**Note** The Multicast control packets are *not* processed when the system memory utilization is more than 90 %. The following message is displayed on the console.

```
*Sep 18 18:21:07.287: %SYS-2-NOMEMORY: No memory available for multicast control packets,
dropping multicast control packets.
Memory usage percentage: 91
```

The system memory utilization may increase when the number of multicast sources and IGMP reports join rate is increased. When 90% of the system memory is used, the IGMP reports are *not* processed and multicast may not function as expected. For the multicast reports to be processed again, decrease the join rate.

## Information About IPv6 Multicast

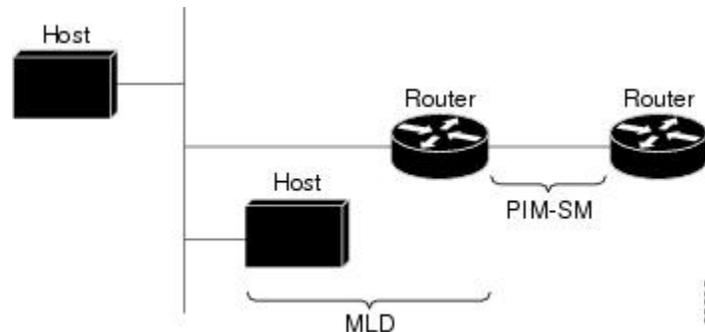
### IPv6 Multicast Routing Implementation

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

- MLD is used by IPv6 devices to discover multicast listeners (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.
  - 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 device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM-SM is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in Source Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address.

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

**Figure 1: IPv6 Multicast Routing Protocols Supported for IPv6**



## Protocol Independent Multicast

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

You can configure IPv6 multicast to use either a PIM- Sparse Mode (SM) or PIM-Source Specific Multicast (SSM) operation, or you can use both PIM-SM and PIM-SSM together in your network.

### 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 devices are involved in each multicast and these devices 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 device 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 device.

As a PIM join travels up the tree, devices 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 device 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 device 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 devices 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

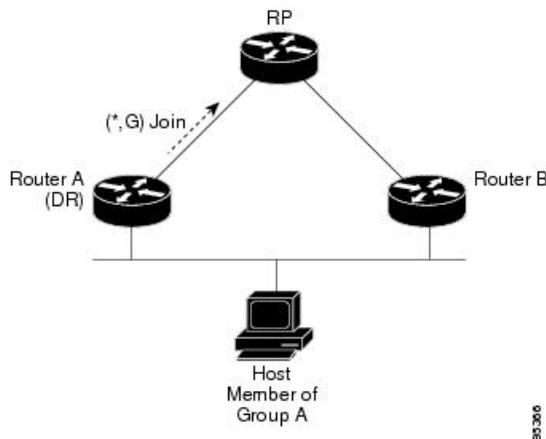
Cisco devices use PIM-SM to forward multicast traffic and follow an election process to select a designated device when there is more than one device on a LAN segment.

The designated router (DR) 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 devices on a LAN, a DR must be elected to avoid duplicating multicast traffic for connected hosts. The PIM device 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 device on the LAN segment (default priority = 1) so that the device with the highest priority will be elected as the DR. If all devices 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. Device A and Device B are connected to a common multiaccess Ethernet segment with Host A as an active receiver for Group A. Only Device A, operating as the DR, sends joins to the RP to construct the shared tree for Group A. If Device 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 devices were assigned the responsibility, the RP would receive duplicate multicast packets and result in wastage of bandwidth.

**Figure 2: Designated Router Election on a Multiaccess Segment**



If the DR should fail, the PIM-SM provides a way to detect the failure of Device A and elect a failover DR. If the DR (Device A) became inoperable, Device B would detect this situation when its neighbor adjacency with Device A timed out. Because Device 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 Device B. Additionally, if Host A were sourcing traffic, Device 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 Device B.



---

**Tip** Two PIM devices 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 device to learn RP information using the multicast group destination address instead of the statically configured RP. For devices that are the RP, the device must be statically configured as the RP.

The device searches for embedded RP group addresses in MLD reports or PIM messages and data packets. On finding such an address, the device learns the RP for the group from the address itself. It then uses this learned RP for all protocol activity for the group. For devices that are the RP, the device 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 devices 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 device 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 devices 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 devices to send PIM join and prune messages to the RP to inform it about group membership. You must configure the RP address on all devices (including the RP device).

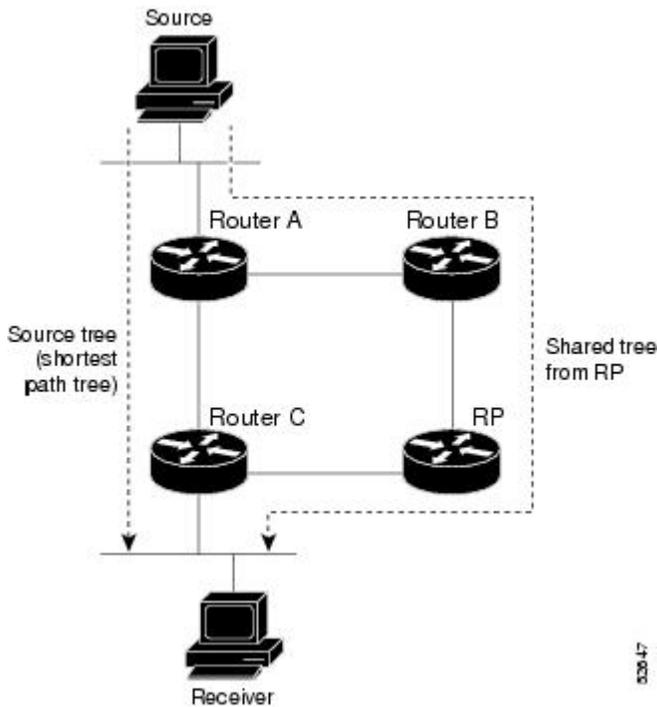
A PIM device can be an RP for more than one group. Only one RP address can be used at a time within a PIM domain for a certain group. The conditions specified by the access list determine for which groups the device is an RP.

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.

## 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 3: Shared Tree and Source Tree (Shortest Path Tree)



If the data threshold warrants, leaf devices 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 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 Device C sends a join message toward the RP.
2. RP puts the link to Device C in its outgoing interface list.
3. Source sends the data; Device A encapsulates the data in the register and sends it to the RP.
4. RP forwards the data down the shared tree to Device C and sends a join message toward the source. At this point, data may arrive twice at Device C, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at the RP, the RP sends a register-stop message to Device A.
6. By default, receipt of the first data packet prompts Device C to send a join message toward the source.
7. When Device C receives data on (S, G), it sends a prune message for the source up the shared tree.
8. RP deletes the link to Device 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 device 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 (DR) 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 device 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 device 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 device has source-tree state (that is, an (S, G) entry is present in the multicast routing table), the device performs the RPF check against the IPv6 address of the source of the multicast packet.
- If a PIM device 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.



---

**Note** To do a RPF check, use the **show ipv6 rpf hostname** or **show ipv6 rpf vrf vrf\_name hostname** command.

---

## IPv6 Multicast: PIM Sparse Mode

IPv6 multicast provides support for intradomain multicast routing using PIM sparse mode (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.

## IPv6 PIM Passive Mode

A device configured with PIM will always send out PIM hello messages to all interfaces enabled for IPv6 multicast routing, even if the device is configured not to accept PIM messages from any neighbor on the LAN.

## IPv6 Multicast: PIM Source-Specific Multicast

The PIM source-specific multicast (SSM) routing protocol supports SSM implementation and is derived from PIM-SM. However, unlike PIM-SM 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.

## IPv6 Source Specific Multicast Mapping

SSM mapping for IPv6 supports both static and dynamic Domain Name System (DNS) mapping for MLD version 1 receivers. This feature allows deployment of IPv6 SSM with hosts that are incapable of providing

MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application. SSM mapping allows the device to look up the source of a multicast MLD version 1 report either in the running configuration of the device or from a DNS server. The device can then initiate an (S, G) join toward the source.

## Selective Packet Discard

Selective Packet Discard (SPD) is a mechanism to manage the process level input queues on the Route Processor (RP). When the router receives bursty traffic, it cannot handle all packets. The input queue is maintained by the hardware interfaces and shared amongst all the sub interfaces. The default input queue size is 75 and is configured per interface using the **hold-queue length {in | out}** command in interface configuration mode. If SPD is not configured, all packets are dropped if the input queue is full when the packet is received.

All packets processed by the router CPU through process switching are queued in the interface input queue. Packets are queued until the queue reaches its maximum length and then additional packets are indiscriminately tail dropped. SPD provides intelligent handling of packets in this queue.

SPD provides preferential treatment during congestion of this interface-to-process-switching queue. As MLD packets fall in the low priority they get dropped during the congestion. To avoid the drops in MLD control packets, increase the below threshold values using the following commands.

- **ipv6 spd queue max-threshold**
- **ipv6 spd queue min-threshold**

Use the **hold-queue length in** command on the interfaces to receive the MLD packets.

# How to Configure IPv6 Multicast

## Enabling IPv6 Multicast Routing

IPv6 multicast 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 device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.

### Before you begin

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 multicast-routing [vrf vrf-name]</b> <b>Example:</b> Device(config)# ipv6 multicast-routing	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device. <ul style="list-style-type: none"> <li>IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. IPv6 multicast-routing needs to be enabled for IPv6 multicast routing to function.</li> </ul>

## 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

	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.

	Command or Action	Purpose
<b>Step 3</b>	<p><b>ipv6 pim</b> [<i>vrf vrf-name</i>] <b>spt-threshold infinity</b> [<i>group-list access-list-name</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1</pre>	Configures when a PIM leaf device joins the SPT for the specified groups.
<b>Step 4</b>	<p><b>ipv6 pim</b> [<i>vrf vrf-name</i>] <b>accept-register</b> {<i>list access-list</i>   <i>route-map map-name</i>}</p> <p><b>Example:</b></p> <pre>Device(config)# ipv6 pim accept-register route-map reg-filter</pre>	Accepts or rejects registers at the RP.
<b>Step 5</b>	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b></p> <pre>Device(config)# interface gigabitethernet 0/1/0</pre>	Specifies an interface type and number, and places the device 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>Device(config-if)# ipv6 pim dr-priority 3</pre>	Configures the DR priority on a PIM device.
<b>Step 7</b>	<p><b>ipv6 pim hello-interval</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Device(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>Device(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>Device(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> [<i>vrf vrf-name</i>] <b>join-prune statistic</b> [<i>interface-type</i>]</p> <p><b>Example:</b></p> <pre>Device# show ipv6 pim join-prune statistic</pre>	Displays the average join-prune aggregation for the most recently aggregated packets for each interface.

# 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. **end**
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

	Command or Action	Purpose
Step 1	<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>
Step 2	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]</b> <b>Example:</b> Device(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.
Step 4	<b>end</b> <b>Example:</b> Device(config-if)# end	Returns to privileged EXEC mode.
Step 5	<b>show ipv6 pim [vrf vrf-name] interface [state-on] [state-off] [type number]</b> <b>Example:</b> Device# show ipv6 pim interface	Displays information about interfaces configured for PIM.

	Command or Action	Purpose
<b>Step 6</b>	<p><b>show ipv6 pim</b> [<i>vrf 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>Device# show ipv6 pim group-map</pre>	Displays an IPv6 multicast group mapping table.
<b>Step 7</b>	<p><b>show ipv6 pim</b> [<i>vrf 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>Device# show ipv6 pim neighbor</pre>	Displays the PIM neighbors discovered by the Cisco IOS software.
<b>Step 8</b>	<p><b>show ipv6 pim</b> [<i>vrf 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>Device# show ipv6 pim range-list</pre>	Displays information about IPv6 multicast range lists.
<b>Step 9</b>	<p><b>show ipv6 pim</b> [<i>vrf vrf-name</i>] <b>tunnel</b> [<i>interface-type interface-number</i>]</p> <p><b>Example:</b></p> <pre>Device# show ipv6 pim tunnel</pre>	Displays information about the PIM register encapsulation and de-encapsulation tunnels on an interface.
<b>Step 10</b>	<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>Device# debug ipv6 pim</pre>	Enables debugging on PIM protocol activity.

## Resetting the PIM Traffic Counters

If PIM malfunctions, or in order to verify that the expected number of PIM packets are received and sent, clear PIM traffic counters. Once the traffic counters are cleared, you can 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
Step 1	<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>
Step 2	<b>clear ipv6 pim [vrf vrf-name] traffic</b> <b>Example:</b> Device# clear ipv6 pim traffic	Resets the PIM traffic counters.
Step 3	<b>show ipv6 pim [vrf vrf-name] traffic</b> <b>Example:</b> Device# show ipv6 pim traffic	Displays the PIM traffic counters.

## 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 mrrib [vrf vrf-name] client [filter] [name {client-name | client-name : client-id}]**
4. **show ipv6 mrrib [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 mrrib [vrf vrf-name] client**
7. **debug ipv6 mrrib [vrf vrf-name] io**
8. **debug ipv6 mrrib proxy**
9. **debug ipv6 mrrib [vrf vrf-name] route [group-name | group-address]**
10. **debug ipv6 mrrib [vrf vrf-name] table**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<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>

	Command or Action	Purpose
<b>Step 2</b>	<p><b>clear ipv6 pim</b> [<i>vrf vrf-name</i>] <b>topology</b> [<i>group-name</i>   <i>group-address</i>]</p> <p><b>Example:</b></p> <pre>Device# clear ipv6 pim topology FF04::10</pre>	Clears the PIM topology table.
<b>Step 3</b>	<p><b>show ipv6 mrib</b> [<i>vrf vrf-name</i>] <b>client</b> [<i>filter</i>] [<i>name</i> {<i>client-name</i>   <i>client-name</i> : <i>client-id</i>}]</p> <p><b>Example:</b></p> <pre>Device# show ipv6 mrib client</pre>	Displays multicast-related information about an interface.
<b>Step 4</b>	<p><b>show ipv6 mrib</b> [<i>vrf vrf-name</i>] <b>route</b> [<i>link-local</i>   <i>summary</i>   [<i>sourceaddress-or-name</i>   *] [<i>groupname-or-address</i> [<i>prefix-length</i>]]]</p> <p><b>Example:</b></p> <pre>Device# show ipv6 mrib route</pre>	Displays the MRIB route information.
<b>Step 5</b>	<p><b>show ipv6 pim</b> [<i>vrf vrf-name</i>] <b>topology</b> [<i>groupname-or-address</i> [<i>sourcename-or-address</i>]   <i>link-local</i>   <i>route-count</i> [<i>detail</i>]]]</p> <p><b>Example:</b></p> <pre>Device# 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> [<i>vrf vrf-name</i>] <b>client</b></p> <p><b>Example:</b></p> <pre>Device# debug ipv6 mrib client</pre>	Enables debugging on MRIB client management activity.
<b>Step 7</b>	<p><b>debug ipv6 mrib</b> [<i>vrf vrf-name</i>] <b>io</b></p> <p><b>Example:</b></p> <pre>Device# 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>Device# 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> [<i>vrf vrf-name</i>] <b>route</b> [<i>group-name</i>   <i>group-address</i>]</p> <p><b>Example:</b></p> <pre>Device# debug ipv6 mrib route</pre>	Displays information about MRIB routing entry-related activity.

	Command or Action	Purpose
<b>Step 10</b>	<b>debug ipv6 mrib [vrf vrf-name] table</b> <b>Example:</b> Device# debug ipv6 mrib table	Enables debugging on MRIB table management activity.

## 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.



**Note** Though IOS supports disabling PIM on an interface, this is not possible on RSP3 platform due to caveat. Ipv6 multicast packets will still get punted to CPU even if PIM is turned off on the interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 pim**

### 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>interface</b> <i>type number</i> <b>Example:</b> Device(config)# interface gigabitethernet 0/1/0	Specifies an interface type and number, and places the device in interface configuration mode.
<b>Step 4</b>	<b>no ipv6 pim</b> <b>Example:</b> Device(config-if)# no ipv6 pim	Turns off IPv6 PIM on a specified interface.

## Disabling Embedded RP Support in IPv6 PIM

A user might want to disable embedded RP support on an interface if all of the devices 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>	<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>no ipv6 pim [vrf vrf-name] rp embedded</b> <b>Example:</b> Device(config)# no ipv6 pim rp embedded	Disables embedded RP support in IPv6 PIM.
<b>Step 4</b>	<b>interface type number</b> <b>Example:</b> Device(config)# interface gigabitethernet 0/1/0	Specifies an interface type and number, and places the device in interface configuration mode.
<b>Step 5</b>	<b>no ipv6 pim</b> <b>Example:</b> Device(config-if)# no ipv6 pim	Turns off IPv6 PIM on a specified interface.

## Configuring IPv6 SSM

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

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

### Before you begin



**Note** To use DNS-based SSM mapping, the device needs to find at least one correctly configured DNS server to which the device can 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. **end**
7. **show ipv6 mld [vrf vrf-name] ssm-map [source-address]**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<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>
Step 2	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 mld [vrf vrf-name] ssm-map enable</b> <b>Example:</b> Device(config)# ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
Step 4	<b>no ipv6 mld [vrf vrf-name] ssm-map query dns</b> <b>Example:</b> Device(config)# no ipv6 mld ssm-map query dns	Disables DNS-based SSM mapping.

	Command or Action	Purpose
<b>Step 5</b>	<b>ipv6 mld [vrf vrf-name] ssm-map static access-list source-address</b>  <b>Example:</b>  Device(config)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1	Configures static SSM mappings.
<b>Step 6</b>	<b>end</b>  <b>Example:</b>  Device(config-if)# end	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ipv6 mld [vrf vrf-name] ssm-map [source-address]</b>  <b>Example:</b>  Device# show ipv6 mld ssm-map	Displays SSM mapping information.

## Configuring PIM Passive/MLD State Limit

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast pim-passive-enable**
4. **ipv6 mld state-limit number**
5. **interface type number**
6. **ipv6 pim passive**
7. **ipv6 mld limit number**
8. **no ipv6 mld router**
9. **show ipv6 mld interface**

### 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.

	Command or Action	Purpose
<b>Step 3</b>	<b>ipv6 multicast pim-passive-enable</b> <b>Example:</b>  Device(config)# ipv6 multicast pim-passive-enable	Enables the PIM passive feature on an IPv6 device.
<b>Step 4</b>	<b>ipv6 mld state-limit <i>number</i></b> <b>Example:</b>  Device(config)# ipv6 mld state-limit 100	(Optional) Specifies maximum number of dynamic MLD groups allowed on a router.
<b>Step 5</b>	<b>interface <i>type number</i></b> <b>Example:</b>  Device(config)# interface GigabitEthernet 1/0/0	Specifies an interface type and number, and places the device in interface configuration mode.
<b>Step 6</b>	<b>ipv6 pim passive</b> <b>Example:</b>  Device(config-if)# ipv6 pim passive	Enables the PIM passive feature on a specific interface.
<b>Step 7</b>	<b>ipv6 mld limit <i>number</i></b> <b>Example:</b>  Device(config-if)# ipv6 mld limit 300	(Optional) Configure the per-interface MLD state limit. You can use this command to limit the dynamic MLD groups joined.
<b>Step 8</b>	<b>no ipv6 mld router</b> <b>Example:</b>  Device(config-if)# no ipv6 mld router	(Optional) Prevents the interface from processing MLD v1/v2 joins sent through it or to prune from a group it has already joined. To enable the interface to start receiving MLD reports again, use <b>ipv6 mld router</b> command.
<b>Step 9</b>	<b>show ipv6 mld <i>interface</i></b> <b>Example:</b>  Device(config-if)# show ipv6 mld interface 1/0/0	(Optional) Displays MLD information about the interface. You can use this command to determine which interface acts as a querier.

## Configuration Examples for IPv6 Multicast

### Example: Enabling IPv6 Multicast Routing

The following example enables multicast routing on all interfaces and also enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.

```
Device> enable
```

```
Device# configure terminal
Device(config)# ipv6 multicast-routing
```

## Example: Configuring PIM Options

The following example sets the DR priority, the PIM hello interval, and the periodic join on the interface.

```
Device(config)# interface gigabitethernet 1/0/0
Device(config)# ipv6 pim hello-interval 60
Device(config)# ipv6 pim dr-priority 3
```

## Example: Configuring PIM

The following example shows how to configure a device 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.

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

## Example: Displaying PIM-SM Information for a Group Range

This example displays information about interfaces configured for PIM:

```
Device# show ipv6 pim interface state-on
```

Interface	PIM	Nbr Count	Hello Intvl	DR Prior
Gi0/1/2	on	0	30	1
Address: FE80::D2C2:82FF:FE17:F392				
DR : this system				
Gi0/1/5	on	1	30	1
Address: FE80::D2C2:82FF:FE17:F395				
DR : FE80::D2C2:82FF:FE17:FAA5				
Loopback0	on	0	30	1
Address: FE80::D2C2:82FF:FE17:F380				
DR : this system				

This example displays an IPv6 multicast group mapping table:

```
Device# 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
```

This example displays information about IPv6 multicast range lists:

```

Device# 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

```

## Example: Displaying IPv6 PIM Topology Information

```

Device# show ipv6 pim topology

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

(*,FF08::1)
SM UP: 00:04:36 JP: Join(00:00:28) Flags:
RP: 8001::1*
RPF: Tunnel1,8001::1*
   Gi0/1/5           00:04:36 fwd      Join(00:03:01)

(3001::5,FF08::1)
SM SPT UP: 00:04:57 JP: Join(never) Flags: KAT(00:02:12) RA
RPF: GigabitEthernet0/1/2,3001::5*
   Gi0/1/5           00:04:36 fwd      Join(00:03:01)

```

Property Type	Property Value	Property Description
.		

## Example: Displaying Information About PIM Traffic

```

Device# show ipv6 pim traffic

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

Valid PIM Packets          Received      Sent
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

```

## Example: Disabling Embedded RP Support in IPv6 PIM

The following example disables embedded RP support on IPv6 PIM:

```

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

```

## Example: IPv6 SSM Mapping

```

Device# 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

Device# 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

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html</a>

### Standards and RFCs

Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

### MIBs

MB	MIBs Link
—	To locate and download MIBs for selected platforms, Cisco IOS 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>

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for IPv6 Multicast PIM

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 IPv6 Multicast PIM**

<b>Feature Name</b>	<b>Releases</b>	<b>Feature Information</b>
IPv6 Multicast PIM	Cisco IOS XE Release 3.14.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M).