Configuring PIM and PIM6

This chapter describes how to configure the Protocol Independent Multicast (PIM) and PIM6 features on Cisco NX-OS devices in your IPv4 and IPv6 networks.

Information About PIM and PIM6

Note Beginning with Cisco NX-OS Release 5.0(2a), Bidirectional Forwarding Detection (BFD) supports PIM. See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees on which packets from multiple sources are forwarded, as well as source distribution trees on which packets from a single source are forwarded. For more information about multicast, see *Information About Multicast*.

Cisco NX-OS supports PIM sparse mode for IPv4 networks (PIM) and for IPv6 networks (PIM6). In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it. You can configure PIM and PIM6 to run simultaneously on a router. You can use PIM and PIM6 global parameters to configure RPs, message packet filtering, and statistics. You can use PIM and PIM6 interface parameters to enable multicast, identify PIM borders, set the PIM hello message interval, and set the designated router (DR) priority. For more information, see *Configuring PIM or PIM6 Sparse Mode*.

Note Cisco NX-OS does not support PIM dense mode.

In Cisco NX-OS, multicast is enabled only after you enable the PIM or PIM6 feature on each router and then enable PIM or PIM6 sparse mode on each interface that you want to participate in multicast. You can configure PIM for an IPv4 network and PIM6 for an IPv6 network. In an IPv4 network, if you have not already enabled IGMP on the router, PIM enables it automatically. In an IPv6 network, MLD is enabled by default. For information about configuring IGMP and MLD, see *Configuring IGMP* and *Configuring MLD*.

Note Beginning with Cisco NX-OS Release 5.2(1) for the Nexus 7000 Series devices, you can configure PIMv4 to run over generic routing encapsulation (GRE) tunnels including outgoing interfaces (OIFs).

You use the PIM and PIM6 global configuration parameters to configure the range of multicast group addresses to be handled by each of the three distribution modes:

- Any Source Multicast (ASM) provides discovery of multicast sources. It builds a shared tree between sources and receivers of a multicast group and supports switching over to a source tree when a new receiver is added to a group. ASM mode requires that you configure an RP.
- Single Source Multicast (SSM) builds a source tree originating at the designated router on the LAN segment that receives a request to join a multicast source. SSM mode does not require you to configure RPs. Source discovery must be accomplished through other means.
- Bidirectional shared trees (Bidir) build a shared tree between sources and receivers of a multicast group but do not support switching over to a source tree when a new receiver is added to a group. Bidir mode requires that you configure an RP. Bidir forwarding does not require source discovery because only the shared tree is used.

You can combine the three modes to cover different ranges of group addresses. For more information, see *Configuring PIM and PIM6*.

For more information about PIM sparse mode and shared distribution trees used by ASM and Bidir modes, see *RFC 4601*.

For more information about PIM SSM mode, see *RFC 3569*.

For more information about PIM Bidir mode, see *draft-ietf-pim-bidir-09.txt*.

Hello Messages

The PIM process begins when the router establishes PIM neighbor adjacencies by sending PIM hello messages to the multicast address 224.0.0.13. Hello messages are sent periodically at the interval of 30 seconds. When all neighbors have replied, the PIM software chooses the router with the highest priority in each LAN segment as the designated router (DR). The DR priority is based on a DR priority value in the PIM hello message. If the DR priority value is not supplied by all routers, or the priorities match, the highest IP address is used to elect the DR.

The hello message also contains a hold-time value, which is typically 3.5 times the hello interval. If this hold time expires without a subsequent hello message from its neighbor, the device detects a PIM failure on that link.

For added security, you can configure an MD5 hash value that the PIM software uses to authenticate PIM hello messages with PIM neighbors.

For information about configuring hello message authentication, see *Configuring PIM or PIM6 Sparse Mode*.

Join-Prune Messages

When the DR receives an IGMP membership report message from a receiver for a new group or source, the DR creates a tree to connect the receiver to the source by sending a PIM join message out the interface toward the rendezvous point (ASM or Bidir mode) or source (SSM mode).The rendezvous point (RP) is the root of a shared tree, which is used by all sources and hosts in the PIM domain in the ASM or the Bidir mode. SSM does not use an RP but builds a shortest path tree (SPT) that is the lowest cost path between the source and the receiver.

When the DR determines that the last host has left a group or source, it sends a PIM prune message to remove the path from the distribution tree.

The routers forward the join or prune action hop by hop up the multicast distribution tree to create (join) or tear down (prune) the path.

Note In this publication, the terms “PIM join message” and “PIM prune message” are used to simplify the action taken when referring to the PIM join-prune message with only a join or prune action.

Join-prune messages are sent as quickly as possible by the software. You can filter the join-prune messages by defining a routing policy. For information about configuring the join-prune message policy, see *Configuring PIM or PIM6 Sparse Mode*.

State Refreshes

PIM requires that multicast entries are refreshed within a 3.5-minute timeout interval. The state refresh ensures that traffic is delivered only to active listeners, and it keeps routers from using unnecessary resources.

To maintain the PIM state, the last-hop DR sends join-prune messages once per minute. State creation applies to both (*, G) and (S, G) states as follows:

- (*, G) state creation example—An IGMP (*, G) report triggers the DR to send a (*, G) PIM join message toward the RP.
- (S, G) state creation example—An IGMP (S, G) report triggers the DR to send an (S, G) PIM join message toward the source.

If the state is not refreshed, the PIM software tears down the distribution tree by removing the forwarding paths in the multicast outgoing interface list of the upstream routers.

Rendezvous Points

A rendezvous point (RP) is a router that you select in a multicast network domain that acts as a shared root for a multicast shared tree. You can configure as many RPs as you like, and you can configure them to cover different group ranges.

Static RP

You can statically configure an RP for a multicast group range. You must configure the address of the RP on every router in the domain.

You can define static RPs for the following reasons:

- To configure routers with the Anycast-RP address
- To manually configure an RP on a device

For information about configuring static RPs, see *Configuring Static RPs*.

BSRs

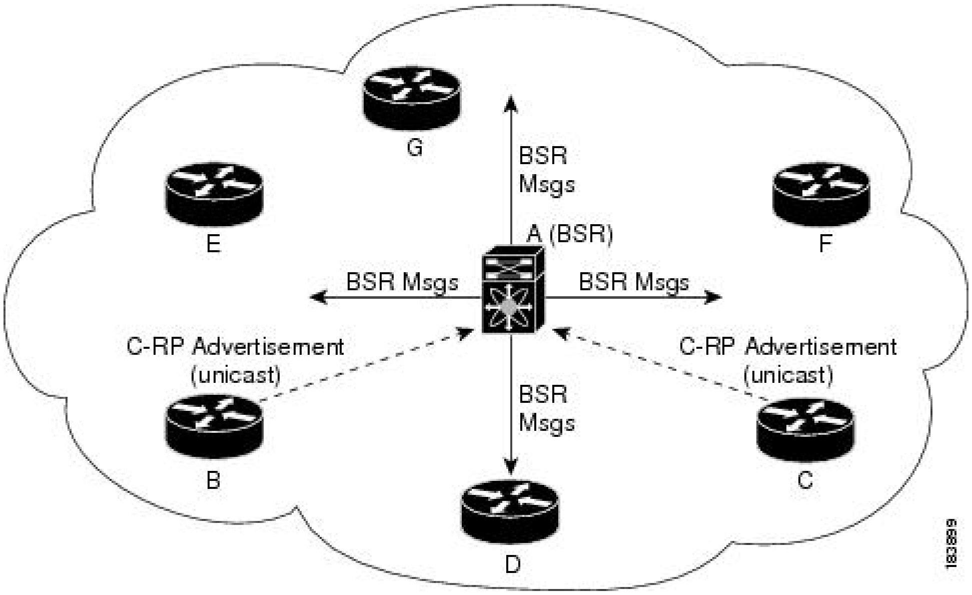
The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs to manage the RPs in the domain. Only one candidate BSR is elected as the BSR for the domain.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

This figure shows the BSR mechanism. Router A, the software-elected BSR, sends BSR messages out all enabled interfaces (shown by the solid lines in the figure). The messages, which contain the RP set, are flooded hop by hop to all routers in the network. Routers B and C are candidate RPs that send their candidate-RP advertisements directly to the elected BSR (shown by the dashed lines in the figure).

The elected BSR receives candidate-RP messages from all the candidate RPs in the domain. The bootstrap message sent by the BSR includes information about all of the candidate RPs. Each router uses a common algorithm to select the same RP address for a given multicast group.

Figure 1: BSR Mechanism



In the RP selection process, the RP address with the best priority is determined by the software. If the priorities match for two or more RP addresses, the software may use the RP hash in the selection process. Only one RP address is assigned to a group.

By default, routers are not enabled to listen or forward BSR messages. You must enable the BSR listening and forwarding feature so that the BSR mechanism can dynamically inform all routers in the PIM domain of the RP set assigned to multicast group ranges.

For more information about bootstrap routers, see *RFC 5059*.

Note The BSR mechanism is a nonproprietary method of defining RPs that can be used with third-party routers.

For information about configuring BSRs and candidate RPs, see *Configuring BSRs*.

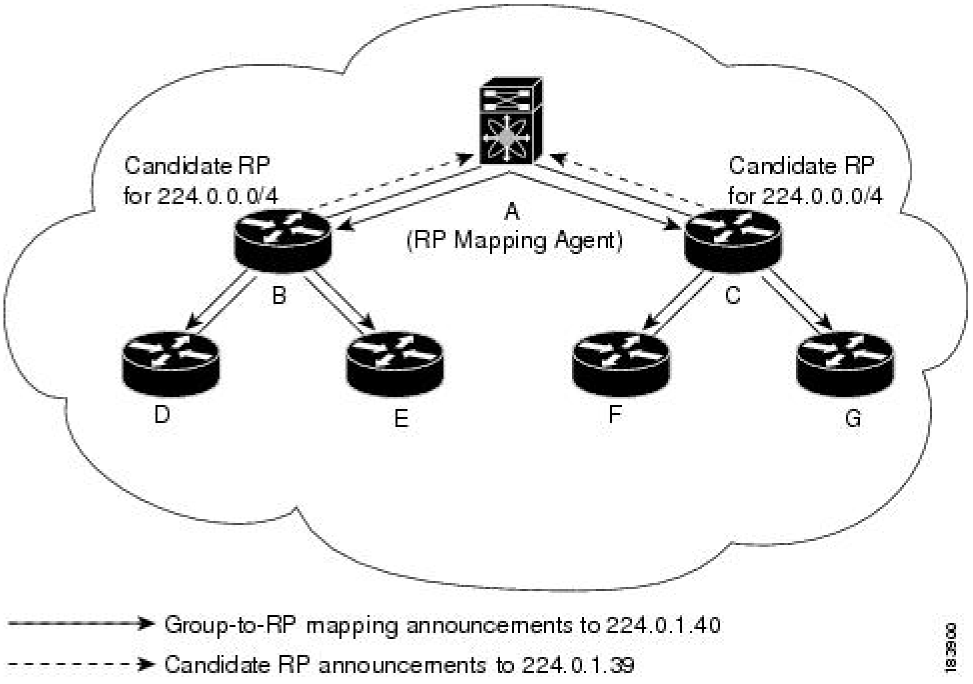
Auto-RP

Auto-RP is a Cisco protocol that was prior to the Internet standard bootstrap router mechanism. You configure Auto-RP by selecting candidate mapping agents and RPs. Candidate RPs send their supported group range in RP-Announce messages to the Cisco RP-Announce multicast group 224.0.1.39. An Auto-RP mapping agent listens for RP-Announce messages from candidate RPs and forms a Group-to-RP mapping table. The mapping agent multicasts the Group-to-RP mapping table in RP-Discovery messages to the Cisco RP-Discovery multicast group 224.0.1.40.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

This figure shows the Auto-RP mechanism. Periodically, the RP mapping agent multicasts the RP information that it receives to the Cisco-RP-Discovery group 224.0.1.40 (shown by the solid lines in the figure).

Figure 2: Auto-RP Mechanism


Candidate RP
for 224.0.0.0/4
Candidate RP
for 224.0.0.0/4
A
(RP Mapping Agent)
B
C
D
E
F
G
Group-to-RP mapping announcements to 224.0.1.40
Candidate RP announcements to 224.0.1.39

By default, routers are not enabled to listen or forward Auto-RP messages. You must enable the Auto-RP listening and forwarding feature so that the Auto-RP mechanism can dynamically inform routers in the PIM domain of the group-to-RP mapping.

Note Auto-RP is not supported for PIM6.

For information about configuring Auto-RP, see *Configuring Auto-RP*.

Multiple RPs Configured in a PIM Domain

This section describes the election process rules when multiple RPs are configured in a PIM domain.

PIM BSR Bootstrap/Auto-RP Mapping-Agent Election Process

This section describes the BSR bootstrap Auto-RP mapping-agent election process.

Bootstrap Router (BSR) Election Process Details

- If the BSR priorities are different, the BSR with the highest priority (highest numerical value) is elected as the BSR router for the PIM domain (see configuration example 1).
  - Configuration example 1—Different BSR-candidate priorities: In this example, the system elects the device labeled N7K-1 as the BSR candidate for the PIM domain because it has the highest priority. The device labeled N7K-2 has the default priority of 64.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0 priority 128

ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0

ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim rp
 PIM RP Status Information for VRF "default"
 BSR: 192.168.1.1*, next Bootstrap message in: 00:00:12,

      priority: 128, hash-length: 30
```

Verification for N7K-2:

```
show ip pim rp
 PIM RP Status Information for VRF "default"
 BSR: 192.168.1.1, uptime: 00:04:27, expires: 00:02:00,
      priority: 128, hash-length: 30
```

- If the BSR priorities are the same, the BSR with the highest BSR-candidate IP address is elected as the BSR router for the PIM domain (see configuration example 2).
    - Configuration example 2—Identical BSR-candidate priorities: In this example, the system elects the device labeled N7K-2 as the BSR for the PIM domain because it has the highest BSR-candidate IP address.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0

ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0

ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim rp
PIM RP Status Information for VRF "default"
 BSR: 192.168.2.1, uptime: 01:45:20, expires: 00:01:54,
         priority: 64, hash-length: 30
```

Verification for N7K-2:

```
show ip pim rp
PIM RP Status Information for VRF "default"
 BSR: 192.168.2.1*, next Bootstrap message in: 00:00:30,
      priority: 64, hash-length: 30
```

Auto-RP Mapping Agent Election Process

- The router with the highest mapping-agent IP address is elected as the mapping agent for the PIM domain. You cannot configure the priority for the Auto-RP mapping agent (see configuration example):
    - Configuration example—Highest IP address: In this example, the system elects the device labeled N7K-2 as the mapping agent for the PIM domain because it has the highest mapping-agent IP address.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim auto-rp mapping-agent loopback0

ip pim auto-rp forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim auto-rp mapping-agent loopback0

ip pim auto-rp forward listen
```

Verification for N7K-1:

```
show ip pim rp
PIM RP Status Information for VRF "default"
 BSR disabled
 Auto-RP RPA: 192.168.2.1, next Discovery message in: 00:00:52
```

Verification for N7K-2:

```
show ip pim rp
PIM RP Status Information for VRF "default"
 BSR disabled
 Auto-RP RPA: 192.168.2.1*, next Discovery message in: 00:00:47
```

PIM RP versus RP Election Process

This table shows the process that the system uses to select the RP for a multicast group if multiple RPs are configured in the network using BSR, Auto-RP, or static RP configurations.

BSR-RP vs. BSR-RP	BSR-RP vs. Static RP	Auto-RP vs. Auto- RP	Auto-RP vs. Static RP
1. Most specific RP group-list	1.Most specific RP group-list	1. Most specific RP group-list	1. Most specific RP group-list
2. Lowest RP priority	2. Highest RP IP address	2. Highest RP IP address	2. Highest RP IP address
3. Highest RP IP address	—	—	—

Note BSR-RP versus Auto-RP is not listed in this table because we recommend that you do not run both simultaneously in the same network.

PIM BSR RP-Candidate Versus BSR RP-Candidate Election Process

- The BSR RP-candidate with the most specific group list is elected as the RP for any multicast addresses specified in its configured group list. The most specific group list takes priority over the BSR RP-candidate priority and the highest BSR RP-candidate IP address (see configuration example 1).
    - Configuration example 1—Most specific group list: In this example, the system elects the device labeled N7K-1 as the RP for all multicast addresses specified in the 224.1.1.0/24 group-list. The system elects the device labeled N7K-2 for the multicast addresses within the less specific 224.0.0.0/4 group list.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.1.1.0/24
ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode
ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.1.1.0/24       ASM       192.168.1.1      -

show ip pim group 224.3.0.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

Verification for N7K-2:

```
show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.1.1.0/24       ASM       192.168.1.1      -

show ip pim group 224.3.0.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1
```

-
- When multiple BSR RP-candidates advertise the same group list (for example, 224.0.0.0/4), the system elects the BSR RP-candidate with the highest priority (lowest numerical value) as the RP for any multicast address specified in its group list (see configuration example 2).
    - Configuration example 2—Identical group list with different RP priorities: In this example, the system elects the device labeled N7K-1 as the RP for all multicast addresses specified in the 224.0.0.0/4 group list because it has the lowest RP-candidate priority. The device labeled N7K-2 has a default priority of 192.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4 priority 10
ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim rp
 PIM RP Status Information for VRF "default"
 BSR: 192.168.2.1, uptime: 00:09:14, expires: 00:01:37,
  priority: 64, hash-length: 30
 Auto-RP disabled
 BSR RP Candidate policy: None
 BSR RP policy: None
 Auto-RP Announce policy: None
 Auto-RP Discovery policy: None

 RP: 192.168.1.1*, (0), uptime: 00:08:15, expires: 00:01:57,
  priority: 10, RP-source: 192.168.2.1 (B), group ranges:
 224.0.0.0/4

 RP: 192.168.2.1, (0), uptime: 00:08:15, expires: 00:01:57,
  priority: 192, RP-source: 192.168.2.1 (B), group ranges:
 224.0.0.0/4

show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.1.1
```

Verification for N7K-2:

```
show ip pim rp
 PIM RP Status Information for VRF "default"
 BSR: 192.168.2.1*, next Bootstrap message in: 00:00:55,
  priority: 64, hash-length: 30
 Auto-RP disabled
 BSR RP Candidate policy: None
 BSR RP policy: None
 Auto-RP Announce policy: None
 Auto-RP Discovery policy: None

 RP: 192.168.1.1, (0), uptime: 00:11:34, expires: 00:02:26,
  priority: 10, RP-source: 192.168.1.1 (B), group ranges:
 224.0.0.0/4

 RP: 192.168.2.1*, (0), uptime: 00:12:21, expires: 00:02:22,
  priority: 192, RP-source: 192.168.2.1 (B), group ranges:
 224.0.0.0/4

show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.1.1      -
```

- When multiple BSR RP-candidates advertise the same group list (for example, 224.0.0.0/4) and are configured with the same BSR RP-candidate priority, the system elects the BSR RP-candidate with the highest IP address as the RP for any multicast address specified in its group list (see configuration example 3).
    - Configuration example 3—Identical group list with identical RP priorities: In this example, the system elects the device labeled N7K-2 as the RP for all multicast addresses specified in the 224.0.0.0/4 group list because it has the highest RP-candidate IP address.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

Verification for N7K-2:

```
show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

PIM BSR RP-Candidate Versus Static RP Election Process

- The RP with the most specific group list is elected as the RP for any multicast addresses specified in its configured group list. The most specific group list takes priority over the highest RP IP address (see configuration example 1). (RP priorities are not applicable when comparing BSR RP-candidates to static RPs.)
  - Configuration example 1—Most specific group list: In this example, the system elects the device labeled N7K-1 as the BSR RP for all multicast addresses specified in the 224.1.1.0/24 group list. The system elects the device labeled N7K-2 as the RP for the multicast addresses within the less specific 224.0.0.0/4 group list because of the static RP statement.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4
ip pim bsr rp-candidate loopback0 group-list 224.1.1.0/24
ip pim forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4

ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.1.1.0/24       ASM       192.168.1.1      -

show ip pim group 224.3.0.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

Verification for N7K-2:

```
show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.1.1.0/24       ASM       192.168.1.1      -

show ip pim group 224.3.0.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

- When a static RP and the BSR RP-candidate advertise the same group list (for example, 224.0.0.0/4), the system elects the system with the highest RP IP address as the RP for any multicast addresses specified in its group list (see configuration example 2).
  - Configuration example 2—Identical RP group list: In this example, the system elects the device labeled N7K-2 as the RP for all multicast addresses specified in the 224.0.0.0/4 group list because it has the highest RP IP address.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim rp-address 192.168.1.1 group-list 224.0.0.0/4

ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim rp-address 192.168.1.1 group-list 224.0.0.0/4
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
224.0.0.0/4        ASM       192.168.2.1
```

Verification for N7K-2:

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
224.0.0.0/4        ASM       192.168.2.1      -
```

- Because you cannot configure a static RP and its default value is 0, the RP priority has no impact. You can configure the BSR RP-candidate with a value between 0 and 255. The system elects the device with the most specific group list. If both devices have the same group list, the system elects the device with the highest RP IP address (see configuration example 3).
    - Configuration example 3—Identical group list and identical RP priorities: In this example, the system elects the device labeled N7K-2 as the RP for all multicast addresses specified in the 224.0.0.0/4 group list because it has the highest RP IP address. The system does not compare RP priorities between BSR RPs and static RPs.

Configuration for N7K-1:

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4 priority 0

ip pim bsr forward listen
```

Configuration for N7K-2:

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4

ip pim bsr forward listen
```

Verification for N7K-1:

```
show ip pim rp
 PIM RP Status Information for VRF "default"
 BSR: 192.168.1.1*, next Bootstrap message in: 00:00:52,
  priority: 64, hash-length: 30
 Auto-RP disabled
 BSR RP Candidate policy: None
 BSR RP policy: None
 Auto-RP Announce policy: None
 Auto-RP Discovery policy: None

 RP: 192.168.1.1*, (0), uptime: 00:01:57, expires: 00:02:25,
 priority: 0, RP-source: 192.168.1.1 (B), group ranges:
  224.0.0.0/4
 RP: 192.168.2.1, (0), uptime: 02:16:09, expires: never,
 priority: 0, RP-source: (local), group ranges:
  224.0.0.0/4

show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

Verification for N7K-2:

```
show ip pim rp
 PIM RP Status Information for VRF "default"
 BSR: 192.168.1.1, uptime: 00:29:47, expires: 00:01:45,
  priority: 64, hash-length: 30
 Auto-RP disabled
 BSR RP Candidate policy: None
 BSR RP policy: None
 Auto-RP Announce policy: None
 Auto-RP Discovery policy: None

 RP: 192.168.1.1, (0), uptime: 00:06:59, expires: 00:02:05,
 priority: 0, RP-source: 192.168.1.1 (B), group ranges:
  224.0.0.0/4
 RP: 192.168.2.1*, (0), uptime: 00:13:15, expires: never,
 priority: 0, RP-source: (local), group ranges:
  224.0.0.0/4

show ip pim group 224.1.1.0
 PIM Group-Range Configuration for VRF "default"
 Group-range        Mode      RP-address       Shared-tree-only range

 224.0.0.0/4        ASM       192.168.2.1      -
```

PIM Auto-RP-Candidate Versus Auto-RP-Candidate Election Process

The auto-RP-candidate election is similar to the BSR RP-candidate election process, but it does not support priorities (see the *PIM BSR RP-Candidate vs. BSR RP-Candidate Election Process*). You cannot configure the priority for an auto-RP. The default value is 0.

PIM Auto-RP-Candidate Versus Static RP Election Process

The auto-RP-candidate versus static RP election uses the same rules as the election process for the BSR RP-candidate versus static RP See *PIM BSR RP-Candidate vs. Static RP Election Process*.

Anycast-RP

Anycast-RP has two implementations: one uses Multicast Source Discovery Protocol (MSDP) and the other is based on*RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM)*. This section describes how to configure PIM Anycast-RP.

You can use PIM Anycast-RP to assign a group of routers, called the Anycast-RP set, to a single RP address that is configured on multiple routers. The set of routers that you configure as Anycast-RPs is called the Anycast-RP set. This method is the only RP method that supports more than one RP per multicast group, which allows you to load balance across all RPs in the set. The Anycast RP supports all multicast groups.

PIM register messages are sent to the closest RP and PIM join-prune messages are sent in the direction of the closest RP as determined by the unicast routing protocols. If one of the RPs goes down, unicast routing ensures these message will be sent in the direction of the next-closest RP.

You must configue PIM on the loopback interface that is used for the PIM Anycast RP.

For more information about PIM Anycast-RP, see *RFC 4610*.

For information about configuring Anycast-RPs, see *Configuring a PIM Anycast-RP Set*.

PIM Register Messages

PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions:

- To notify the RP that a source is actively sending to a multicast group.
- To deliver multicast packets sent by the source to the RP for delivery down the shared tree.

The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:

- The RP has no receivers for the multicast group being transmitted.
- The RP has joined the SPT to the source but has not started receiving traffic from the source.

You can use the **ip pim register-source** command to configure the IP source address of register messages when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation might occur if the source address is filtered so that the packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address will fail to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures.

This example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

Note In Cisco NX-OS, PIM register messages are rate limited to avoid overwhelming the RP.

You can filter PIM register messages by defining a routing policy. For information about configuring the PIM register message policy, see the *Configuring Shared Trees Only for ASM*.

Designated Routers

In PIM ASM and SSM modes, the software chooses a designated router (DR) from the routers on each network segment. The DR is responsible for forwarding multicast data for specified groups and sources on that segment.

The DR for each LAN segment is determined as described in the *Hello Messages*.

In ASM mode, the DR is responsible for unicasting PIM register packets to the RP. When a DR receives an IGMP membership report from a directly connected receiver, the shortest path is formed to the RP, which may or may not go through the DR. The result is a shared tree that connects all sources transmitting on the same multicast group to all receivers of that group.

In SSM mode, the DR triggers (*, G) or (S, G) PIM join messages toward the RP or the source. The path from the receiver to the source is determined hop by hop. The source must be known to the receiver or the DR.

For information about configuring the DR priority, see the *Configuring PIM or PIM6 Sparse Mode*.

Designated Forwarders

In PIM Bidir mode, the software chooses a designated forwarder (DF) at RP discovery time from the routers on each network segment. The DF is responsible for forwarding multicast data for specified groups on that segment. The DF is elected based on the best metric from the network segment to the RP.

If the router receives a packet on the RPF interface toward the RP, the router forwards the packet out all interfaces in the OIF-list. If a router receives a packet on an interface on which the router is the elected DF for that LAN segment, the packet is forwarded out all interfaces in the OIF-list except the interface that it was received on and also out the RPF interface toward the RP.

Note Cisco NX-OS does not support PIM Bidir mode on F2 modules.

Note Cisco NX-OS puts the RPF interface into the OIF-list of the MRIB, but not in the OIF-list of the MFIB.

ASM Switchover from Shared Tree to Source Tree

Note Cisco NX-OS puts the RPF interface into the OIF-list of the MRIB, but not in the OIF-list of the MFIB.

In ASM mode, the DR that is connected to a receiver switches over from the shared tree to the shortest-path tree (SPT) to a source unless you configure the PIM parameter to use shared trees only. For information about configuring the use of shared trees only, see the *Configuring Shared Trees Only for ASM*.

During the switchover, messages on the SPT and shared tree may overlap. These messages are different. The shared tree messages are propagated upstream toward the RP, while SPT messages go toward the source.

For information about SPT switchovers, see the "Last-Hop Switchover" to the SPT section in *RFC 4601*.

ECMP Multicast Load Splitting Based on Source Group and Next-Hop Address Overview

The Advanced Multicast Multipath Support feature adds support for Equal Cost Multipath (ECMP) multicast load splitting based on source, group, and next-hop address. This feature enables multicast traffic from devices that send many streams to groups or that broadcast many channels, such as IPTV servers or MPEG video servers, to be more effectively load split across equal-cost paths.

Configuring ECMP multicast load splitting based on source, group, and next-hop address enables a more complex hash, the next-hop-based S-G-hash algorithm, which is based on source, group, and next-hop address. The next-hop-based S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. Unlike the S-hash and basic S-G-hash algorithms, the hash mechanism used by the next-hop-based S-G-hash algorithm is not subject to polarization.

Note The next-hop-based S-G-hash algorithm in IPv4 multicast is the same algorithm used in IPv6 ECMP multicast load splitting, which, in turn, utilizes the same hash function used for PIM-SM bootstrap device (BSR).

The next-hop-based hash mechanism does not produce polarization and also maintains better RPF stability when paths fail. These benefits come at the cost that the source or RP IP addresses cannot be used to reliably predict and engineer the outcome of load splitting when the next-hop-based S-G-hash algorithm is used. Because many customer networks have implemented equal-cost multipath topologies, the manual engineering of load splitting, thus, is not a requirement in many cases. Rather, it is more of a requirement that the default behavior of IP multicast be similar to IP unicast; that is, it is expected that IP multicast use multiple equal-cost paths on a best-effort basis. Load splitting for IPv4 multicast, therefore, could not be enabled by default because of the anomaly of polarization.

Note Load splitting for CEF unicast also uses a method that does not exhibit polarization and likewise cannot be used to predict the results of load splitting or engineer the outcome of load splitting.

The next-hop-based hash function avoids polarization because it introduces the actual next-hop IP address of PIM neighbors into the calculation, so the hash results are different for each device, and in effect, there is no problem of polarization. In addition to avoiding polarization, this hash mechanism also increases stability of the RPF paths chosen in the face of path failures. Consider a device with four equal-cost paths and a large number of states that are load split across these paths. Suppose that one of these paths fails, leaving only three available paths. With the hash mechanism used by the polarizing hash mechanisms (the hash mechanism used by the S-hash and basic S-G-hash algorithms), the RPF paths of all states would likely reconverge and thus change between those three paths, especially those paths that were already using one of those three paths. These states, therefore, may unnecessarily change their RPF interface and next-hop neighbor. This problem exists simply because the chosen path is determined by taking the total number of paths available into consideration by the algorithm, so once a path changes, the RPF selection for all states is subject to change too. For the next-hop-based hash mechanism, only the states that were using the changed path for RPF would need to reconverge onto one of the three remaining paths. The states that were already using one of those paths would not change. If the fourth path came back up, the states that initially used it would immediately reconverge back to that path without affecting the other states.

Note The next-hop-based S-G-hash algorithm ignores bidir-PIM groups.

Administratively Scoped IP Multicast

The administratively scoped IP multicast method allows you to set boundaries on the delivery of multicast data. For more information, see *RFC 2365*.

You can configure an interface as a PIM boundary so that PIM messages are not sent out that interface. For information about configuring the domain border parameter, see the *Configuring PIM or PIM6 Sparse Mode*.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value. For more information, see the *Configuring Shared Trees Only for ASM*.

Bidirectional Forwarding Detection for PIM

Beginning with Cisco NX-OS Release 5.0(2a), Bidirectional Forwarding Detection (BFD) allows the system to rapidly detect failures in a network. See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*, for more information about BFD.

In PIM, a link or neighbor group failure is detected when the hold-time, which is set as part of the hello interval, expires. However, BFD provides a more efficient method to detect a failure. This protocol establishes a session between the two endpoints over a link and uses the forwarding engine. When BFD is enabled, the PIM process attempts to add a BFD session as each neighbor is discovered. If a BFD session already exists, no duplicate is created but PIM receives a callback that contains the state of the BFD session. You can enable BFD for PIM per VRF or per interface.

PIM removes the BFD session when you disable BFD for that VRF or interface, the interface is no longer a PIM interface, or the neighboring BFD session goes down.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. Within each VDC, multiple virtual routing and forwarding (VRF) instances can be defined. For each VRF in a VDC in the system, independent multicast system resources are maintained, including the MRIB and M6RIB.

You can use the PIM and PIM6 **show** commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

For information about configuring VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Support for Graceful Restart PIM

The Support for Graceful Restart protocol independent multicast (PIM) feature is a multicast High Availability (HA) enhancement that improves the convergence of multicast-routes (mroutes) after a Route Processor (RP) switchover. In the event of an RP switchover, the support for Graceful Restart PIM feature utilizes the

Generation ID (GenID) value (defined in RFC 4601) as a mechanism to trigger adjacent PIM neighbors on an interface to send PIM join messages for all (*, G) and (S, G) states that use that interface as a reverse path forwarding (RPF) interface. This mechanism enables PIM neighbors to immediately reestablish those states on the newly active RP.

Prerequisites for Graceful Restart PIM

All Protocol Independent Multicast (PIM) neighbors must be compliant with RFC 4601 and be able to process Generation ID (GenID) differences in PIM hello messages.

Information About Graceful Restart PIM

Generation IDs

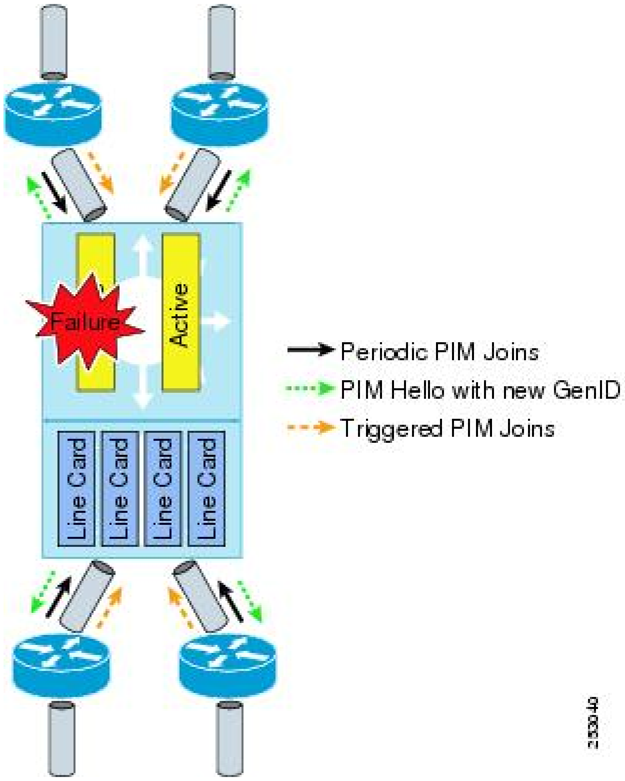
A Generation ID (GenID) is a randomly generated 32-bit value that is regenerated each time protocol independent multicast (PIM) forwarding is started or restarted on an interface. In order to process the GenID value in PIM hello messages, PIM neighbors must be running Cisco software with an implementation of PIM that is compliant with RFC 4601.

Note PIM neighbors that are not compliant with RFC 4601 and are unable to process GenID differences in PIM hello messages will ignore the GenIDs.

Graceful Restart PIM Functional Overview

The figure illustrates the operations that occur after a Route Processor (RP) switchover on devices that support the support for Graceful Restart protocol independent multicast (PIM) feature.

Figure 3: Operation of Graceful Restart PIM during an RP Switchover



The mechanics of the support for Graceful Restart PIM feature are as follows:

- In steady state, PIM neighbors exchange periodic PIM hello messages.
- An active RP receives PIM joins periodically to refresh multicast-route (mroute) states.
- When an active RP fails, the standby RP takes over to become the new active RP.
- The new active RP then modifies the Generation ID (GenID) value and sends the new GenID in PIM hello messages to adjacent PIM neighbors.
- Adjacent PIM neighbors that receive PIM hello messages on an interface with a new GenID send graceful restart PIM for all (*, G) and (S, G) mroutes that use that interfaces as an RPF interface.
- Those mroute states are then immediately reestablished on the newly active RP.

Graceful Restart PIM and Multicast Traffic Flow

Multicast traffic flow on PIM neighbors is not affected if the multicast traffic detects support for Graceful Restart PIM or PIM hello message from a node with the failing RP within the default PIM hello hold-time interval. Multicast traffic flow on a failing RP is not affected if it is Non-Stop Forwarding (NSF) capable.

⚠

Caution The default PIM hello hold-time interval is 3.5 times the PIM hello period. Multicast High Availability (HA) operations may not function as per design if you configure PIM hello interval with a value lower than the default value of 30 seconds.

Additional References for Graceful Restart PIM

RFCs

RFC	Title
RFC 4601	Protocol Independent Multicast - Sparse Mode (PIM-SM)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

High Availability

For information about high availability, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*.

Prerequisites for PIM and PIM6

PIM and PIM6 have the following prerequisites:

- You are logged onto the device.
- You are in the correct virtual device context (VDC). A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.
- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

Guidelines and Limitations for PIM and PIM6

PIM and PIM6 have the following configuration guidelines and limitations:

- PIM must be configured on all Layer 3 interfaces between sources, receivers, and rendezvous points (RPs).

- Cisco NX-OS PIMv4 do not support route-map configuration with RP-Type. You can only configure Group Address, Source Address, and RP-address in the route-map.
- Tunnel interfaces do not support PIM until Cisco NX-OS Release 5.2(1). Beginning with Release 5.2(1), you can configure multicast on generic routing encapsulation (GRE) tunnel interfaces.
- The Cisco NX-OS software does not support multicast on a GRE tunnel interface that is in a different virtual routing and forwarding (VRF) instance than the VRF of the transport interface.
- Cisco NX-OS PIM and PIM6 do not interoperate with any version of PIM dense mode or PIM sparse mode version 1.
- Do not configure both Auto-RP and BSR protocols in the same network.
- Configure candidate RP intervals to a minimum of 15 seconds.
- If a device is configured with a BSR policy that should prevent it from being elected as the BSR, the device ignores the policy. This behavior results in the following undesirable conditions:
    - If a device receives a BSM that is permitted by the policy, the device, which incorrectly elected itself as the BSR, drops that BSM so that routers downstream fail to receive it. Downstream devices correctly filter the BSM from the incorrect BSR so that these devices do not receive RP information.
    - A BSM received by a BSR from a different device sends a new BSM but ensures that downstream devices do not receive the correct BSM.
- F2-Series modules do not support any form of IPv4 or IPv6 tunnels.
- Beginning with Release 5.x, using BFD for PIM to support fast failure detection is recommended.
- Default values for the PIM hello interval are recommended and should not be modified.

Note Aggressive PIM timers have been tested and can be supported in deployments where PIM timers must be modified. However this testing was limited and SSO/ISSU cannot be guaranteed in such a deployment. For more information, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide.*

- Cisco NX-OS PIM and PIM6 do not support Bidir PIM or SSM on vPCs.
- PIM adjacency with a vPC leg or with a router behind a vPC is not supported.

  A PIM adjacency between an Switched Virtual Interface (SVI) on a vPC VLAN (a VLAN that is carried on a vPC Peer-Link) and a downstream device is not supported; this configuration can result in dropped multicast packets. If a PIM neighbor relationship is required with a downstream device, a physical Layer 3 interface must be used on the Nexus switches instead of a vPC SVI.

  For SVIs on vPC Vlans, only one PIM adjacency is supported - which is with the vPC Peer Switch. PIM adjacencies over the VPC Peer-Link with devices other than the VPC Peer Switch for the vPC-SVI are NOT supported.
- Beginning with Release 7.1, PIM Bidir mode is not supported for VDCs that have the F2 Module. Bidir mode is supported on F2E or F2E with F3 modules on the same VDC.

- Use the **ip igmp static-oif** command on a Layer 3 interface of Cisco Nexus device to force the interface getting populated as an Outgoing Interface List (OIL). Do not use the **ip igmp join-group** command for this purpose.
- Multicast works on periodic joins/prune and depending on the topology and number of routers in the network, S,G state takes time to expire.
- The `sprase-mode` must be enabled by using the **ip pim sparse-mode** command on loopback interfaces that are configured as PIM rendezvous points.
- The interface that is used to configure a PIM RP (whether static, BSR or Auto-RP) must have **ip** [**v6**] **pim sparse-mode**.

Default Settings

Table 1: Default PIM and PIM6 Parameters

Parameters	Default
Use shared trees only	Disabled
Flush routes on restart	Disabled
Log Neighbor changes	Disabled
Auto-RP message action	Disabled
BSR message action	Disabled
SSM multicast group range or policy	232.0.0.0/8 for IPv4 and FF3x::/96 for IPv6
PIM sparse mode	Disabled
Designated router priority	0
Hello authentication mode	Disabled
Domain border	Disabled
RP address policy	No message filtering
PIM register message policy	No message filtering
BSR candidate RP policy	No message filtering
BSR policy	No message filtering
Auto-RP mapping agent policy	No message filtering
Auto-RP RP candidate policy	No message filtering
Join-prune policy	No message filtering
Neighbor adjacency policy	Become adjacent with all PIM neighbors

Parameters	Default
BFD	Disabled

Configuring PIM and PIM6

You can configure both PIM and PIM6 on the same router. You configure either PIM or PIM6 for each interface, depending on whether that interface is running IPv4 or IPv6.

Note Cisco NX-OS supports only PIM sparse mode version 2. In this publication, “PIM” refers to PIM sparse mode version 2.

You can configure separate ranges of addresses in the PIM or PIM6 domain using the multicast distribution modes described in the table below.

Multicast Distribution Mode	Requires RP Configuration	Description
ASM	Yes	Any source multicast
Bidir	Yes	Bidirectional shared trees
SSM	No	Single source multicast
RPF routes for multicast	No	RPF routes for multicast

PIM and PIM6 Configuration Tasks

The following steps configure PIM and PIM6.

1. From the multicast distribution modes, select the range of multicast groups that you want to configure in each mode.
2. From the multicast distribution modes, select the range of multicast groups that you want to configure in each mode.
3. Enable the PIM and PIM6 features.
4. Follow the configuration steps for the multicast distribution modes that you selected in Step 1.
    - For ASM or Bidir mode, see the *Configuring ASM and Bidir*.
    - For SSM mode, see the *Configuring SSM*.
    - For RPF routes for multicast, see the *Configuring RPF Routes for Multicast*.
5. Configure message filtering.

Note The CLI commands used to configure PIM or PIM6 differ as follows:

- Commands begin with **ip pim for PIM** and begin with **ipv6 pim for PIM6**
- Commands begin with **show ip pim** for PIM and begin with **show ipv6 pim** for PIM6.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Enabling the PIM and PIM6 Features

Before you can access the PIM or PIM6 commands, you must enable the PIM or PIM6 feature.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature pim** **Example:** `switch(config)# feature pim`	Enables PIM. By default, PIM is disabled.
Step 3	**feature pim6** **Example:** `switch(config)# feature pim6`	Enables PIM6. By default, PIM6 is disabled.
Step 4	**show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	(Optional) Shows the running-configuration information for PIM, including the **feature** command.
Step 5	**show running-configuration pim6** **Example:** `switch(config)# show running-configuration pim6`	(Optional) Shows the running-configuration information for PIM6, including the **feature** command.
Step 6	**copy running-config startup-config** **Example:**	(Optional) Saves configuration changes.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Configuring PIM or PIM6 Sparse Mode Parameters

You configure PIM or PIM6 sparse mode on every device interface that you want to participate in a sparse mode domain. You can configure the sparse mode parameters described in the table below.

Table 2: PIM and PIM6 Sparse Mode Parameters

Parameter	Description
Global to the device	
Auto-RP message action	Enables listening and forwarding of Auto-RP messages. The default is disabled, which means that the router does not listen or forward Auto-RP messages unless it is configured as a candidate RP or mapping agent. **Note** PIM6 does not support the Auto-RP method.
BSR message action	Enables listening and forwarding of BSR messages. The default is disabled, which means that the router does not listen or forward BSR messages unless it is configured as a candidate RP or BSR candidate.
Bidir RP limit	Configures the number of Bidir RPs that you can configure for IPv4 and IPv6. The maximum number of Bidir RPs supported per VRF for PIM and PIM6 combined cannot exceed 8. Values range from 0 to 8. The default is 6 for IPv4 and 2 for IPv6.
Register rate limit	Configures the IPv4 or IPv6 register rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Initial holddown period	Configures the IPv4 or IPv6 initial holddown period in seconds. This holddown period is the time it takes for the MRIB to come up initially. If you want faster convergence, enter a lower value. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Per device interface	
PIM sparse mode	Enables PIM or PIM6 on an interface.

Parameter	Description
Designated router priority	Sets the designated router (DR) priority that is advertised in PIM hello messages on this interface. On a multiaccess network with multiple PIM-enabled routers, the router with the highest DR priority is elected as the DR router. If the priorities match, the software elects the DR with the highest IP address. The DR originates PIM register messages for the directly connected multicast sources and sends PIM join messages toward the rendezvous point (RP) for directly connected receivers. Values range from 1 to 4294967295. The default is 1.
Hello authentication mode	Enables an MD5 hash authentication key, or password, in PIM hello messages on the interface so that directly connected neighbors can authenticate each other. The PIM hello messages are IPsec encoded using the Authentication Header (AH) option. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The authentication key can be up to 16 characters. The default is disabled. **Note** PIM6 does not support hello authentication.
Hello interval	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000. **Note** See the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide* for the verified range of this parameter and associated PIM neighbor scale.
Domain border	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. **Note** PIM6 does not support the Auto-RP method.

Parameter	Description
Neighbor policy	Configures which PIM neighbors to become adjacent to based on a route-map policy[1] where you can specify IP addresses to become adjacent to with the **match ip[v6] address** command. If the policy name does not exist, or no IP addresses are configured in a policy, adjacency is established with all neighbors. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator.

[1] To configure route-map policies, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Configuring PIM Sparse Mode Parameters

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim auto-rp** {**listen** [**forward**] **forward** [**listen**]}
	Example:
	`switch(config)# ip pim auto-rp listen`
		(Optional) Enables listening or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen to or forward Auto-RP messages.

Step 3	**ip pim bsr** {**listen** [**forward**] **forward** [**listen**]}
	Example:
	`switch(config)# ip pim bsr forward`
		(Optional) Enables listening or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen to or forward Auto-RP messages.

Step 4	**show ip pim rp** [*ip-prefix*] [**forward** | *vrf* [**vrf-name** | **all**] **Example:** `switch(config)# show ip pim rp`	(Optional) Enables listening or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen to or forward Auto-RP messages.
Step 5	**ip pim bidir-rp-limit** *limit* **Example:** `switch(config)# ip pim bidir-rp-limit 4`	(Optional) Specifies the number of Bidir RPs that you can configure for IPv4. The maximum number of Bidir RPs supported per VRF for PIM and PIM6 combined cannot exceed 8. Values range from 0 to 8. The default is 6.

	Command or Action	Purpose
Step 6	**ip pim register-rate-limit** *rate* **Example:** `switch(config)# ip pim register-rate-limit 1000`	(Optional) Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 7	[**ip** | **ipv4**] **routing multicast holddown** *holddown-period* **Example:** `switch(config)# ip routing multicast holddown 100`	(Optional) Configures the initial holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 8	**show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	(Optional) Displays PIM running-configuration information, including the Bidir RP limit and register rate limit.

Step 9	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as ethernet slot/port.

Step 10	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 11	**ip pim dr-priority** *priority* **Example:** `switch(config-if)# ip pim dr-priority 192`	(Optional) Sets the designated router (DR) priority that is advertised in PIM hello messages. Values range from 1 to 4294967295. The default is 1.
Step 12	**ip pim hello-authentication ah-md5** *auth-key* **Example:** `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	(Optional) Enables an MD5 hash authentication key in PIM hello messages. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The key can be up to 16 characters. The default is disabled.
Step 13	**ip pim hello-interval** *interval* **Example:**	(Optional) Configures the interval at which hello messages are sent in milliseconds. The

	Command or Action	Purpose
	`switch(config-if)# ip pim hello-interval 25000`	range is from 1000 to 18724286. The default is 30000. **Note** Before Cisco NX-OS Release 5.2(1), the minimum value was 1 millisecond.
Step 14	**ip pim border** **Example:** `switch(config-if)# ip pim border`	(Optional) Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. **Note** When you use **ip pim border** command, the PIM border starts to work as a first-hop router under certain conditions. For information about PIM Multicast Border Router, see RFC 4601.
Step 15	**ip pim neighbor-policy** *policy-name* **Example:** `switch(config-if)# ip pim neighbor-policy my_neighbor_policy`	(Optional) Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. (Optional) Configures which PIM neighbors to become adjacent to based on a route-map policy with the **match ip address** command. The policy name can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator.
Step 16	**show ip pim interface** [*interface* | **brief**] [**vrf** [*vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	(Optional) Displays PIM interface information.
Step 17	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes. (Optional) Configures which PIM neighbors to become adjacent to based on a route-map policy with the **match ip address** command. The policy name can be up to 63 characters. The default is to become adjacent with all PIM neighbors.

Configuring PIM6 Sparse Mode Parameters

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ipv6 pim bsr**{*listen*[*forward*] | *forward*[*listen*]}
	Example:
	`switch(config)# ip pim auto-rp listen`
		(Optional) Enables listening or forwarding of BSR messages. The default is disabled, which means that the software does not listen or forward BSR messages.

Step 3	**show ipv6 pim rp** [*ipv6-prefix*][**vrf***vrf-name*|**all**] **Example:** `switch(config)# show ipv6 pim rp`	(Optional) Displays PIM6 RP information, including BSR listen and forward states.
Step 4	**ipv6 pim bidir-rp-limit** *limit* **Example:** `switch(config)# ipv6 pim bidir-rp-limit 4`	(Optional) Specifies the number of Bidir RPs that you can configure for IPv6. The maximum number of Bidir RPs supported per VRF for PIM and PIM6 combined cannot exceed 8. Values range from 0 to 8. The default is 2.
Step 5	**ipv6 pim register-rate-limit** *rate* **Example:** `switch(config)# ipv6 pim register-rate-limit 1000`	(Optional) Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 6	**ipv6 routing multicast holddown** *holddown-period* **Example:** `switch(config)# ipv6 routing multicast holddown 100`	(Optional) Configures the initial holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 7	**show running-configuration pim6** **Example:** `switch(config)# show running-configuration pim6`	(Optional) Displays PIM6 running-configuration information, including the Bidir RP limit and register rate limit.

Step 8	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

	Command or Action	Purpose
Step 9	**ipv6 pim sparse-mode** **Example:** `switch(config-if)# ipv6 pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 10	**ipv6 pim dr-priority** *priority* **Example:** `switch(config-if)# ipv6 pim dr-priority 192`	(Optional) Sets the designated router (DR) priority that is advertised in PIM6 hello messages. Values range from 1 to 4294967295. The default is 1.
Step 11	**ipv6 pim hello-interval** *interval* **Example:** `switch(config-if)# ipv6 pim hello-interval 25000`	(Optional) Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000. **Note** Before Cisco NX-OS Release 5.2(1), the minimum value was 1 millisecond.
Step 12	**ipv6 pim border** **Example:** `switch(config-if)# ipv6 pim border`	(Optional) Enables the interface to be on the border of a PIM6 domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. **Note** Before Cisco NX-OS Release 5.2(1), the minimum value was 1 millisecond.
Step 13	**ipv6 pim neighbor-policy** *policy-name* **Example:** `switch(config-if)# ip pim border`	(Optional) Configures which PIM6 neighbors to become adjacent to based on a route-map policy with the **match ipv6 address** command. The policy name can be up to 63 characters. The default is to become adjacent with all PIM6 neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator.
Step 14	**show ipv6 pim interface** [*interface* | brief] [**vrf**vrf-name |**all**] **Example:** `switch(config-if)# show ipv6 pim interface`	(Optional) Displays PIM6 interface information.
Step 15	**copy running-config startup-config** **Example:**	(Optional) Saves configuration changes.

	Command or Action	Purpose
	`switch(config-if)# copy running-config startup-config`	

IGMP Querier

IGMP Querier Overview

The IGMP Querier feature supports the sending of Internet Group Management Protocol (IGMP) queries from a router only if the router is a multicast (PIM)-enabled) router. IGMP router functionality will be enabled only when PIM is enabled on the interface. IGMP router functionality will be disabled when PIM is disabled on the interface. If IGMP router functionality is enabled and PIM is disabled subsequently, then the router functionality will be disabled.

Enabling IGMP Querier

Perform this task to enable the sending of IGMP queries from a router only if the router is a multicast (PIM-enabled) router.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** `switch(config)# interface Ethernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 3	**ip pim sparse-mode**] **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse-mode on an interface.

Step 4	**end**
	Example:
	`switch(config-if)# exit`
		Enter this command to go to privileged EXEC mode.

Step 5	**show ip igmp interface** **Example:** `switch# show ip igmp interface`	(Optional) Displays multicast-related information (including information on the IGMP querier) for an interface.

Example: Enabling IGMP Querier

The following example shows how to enable IGMP Querier:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
switch(config-if)#end
switch# show ip igmp interface

IGMP Interfaces for VRF "default", count: 2 Ethernet2/1, Interface status:
protocol-up/link-up/admin-up
  IP address: 10.11.11.1, IP subnet: 10.11.11.0/24
  Active querier: 10.11.11.1, version: 2, next query sent in: 00:01:57
  Membership count: 1
.
.
```

Configuring ASM and Bidir

Any Source Multicast (ASM) and bidirectional shared trees (Bidir) are multicast distribution modes that require the use of RPs to act as a shared root between sources and receivers of multicast data.

To configure ASM or Bidir mode, you configure sparse mode and the RP selection method, where you indicate the distribution mode and assign the range of multicast groups.

Note Bidir mode is not supported for vPCs. For more information about vPCs, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

Configuring Static RPs

You can configure an RP statically by configuring the RP address on every router that participates in the PIM domain.

Note We recommend that the RP address uses the loopback interface and also the interface with the RP address must have **ip pim sparse-mode** enabled.

You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command.

Beginning with Cisco NX-OS Release 5.1(3), the **ip pim rp-address** command has been enhanced with the following functionalities:

- Added the prefix-list method of configuration in addition to existing route-map method.
- Added support for policy actions (route-map or prefix-list).

Note Cisco NX-OS always uses the longest-match prefix to find the RP. So, the behavior is the same irrespective of the position of the group prefix in the route map or in the prefix list.

The following example configuration produces the same output using Cisco NX-OS (231.1.1.0/24 is always denied irrespective of the sequence number):

```
ip prefix-list plist seq 10 deny 231.1.1.0/24
ip prefix-list plist seq 20 permit 231.1.0.0/16
ip prefix-list plist seq 10 permit 231.1.0.0/16
ip prefix-list plist seq 20 deny 231.1.1.0/24
```

This behavior differs from Cisco IOS. See the *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*, behavior for more samples for the **ip pim rp-address** command.

Configuring Static RPs (PIM)

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* | **route-map** *policy-name*] [**bidir**]
	Example:
	`switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`
	Example:
	`switch(config)# ip pim rp-address 192.0.2.34 group-list 224.128.0.0/9 bidir`
		Configures a PIM6 static RP address for a multicast group range. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The mode is ASM unless you specify the **bidir** keyword. The default group range is ff00::0/8.
		Example 1 configures PIM6 ASM mode for the specified group range.
		Example 2 configures PIM6 Bidir mode for the specified group range.

Step 3	**show ip pim group-range** *ipv6-prefix*| **vrf** *vrf-name* **all** **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM6 RP information, including BSR listen and forward states.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Static RPs (PIM6)

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* | **route-map** *policy-nsmr*] [**bidir**]
	Example:
	`switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/24`
	Example:
	`switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::2 group-list ff1e:abcd:def2::0/96 bidir`
		Configures a PIM6 static RP address for a multicast group range. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The mode is ASM unless you specify the **bidir** keyword. The default group range is ff00::0/8.
		Example 1 configures PIM6 ASM mode for the specified group range.
		Example 2 configures PIM6 Bidir mode for the specified group range.

Step 3	**show ipv6 pim rp** *ipv6-prefix*|**vrf***vrf-name***all** **Example:** `switch(config)# show ipv6 pim group-range`	(Optional) Displays PIM6 modes and group ranges.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# show ipv6 pim group-range`	(Optional) Displays PIM6 modes and group ranges.

Configuring BSRs

You configure BSRs by selecting candidate BSRs and RPs.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

You can configure a candidate BSR with the arguments described on the Table below.

Table 3: Candidate BSR Arguments

Argument	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.

Argument	Description
hash-length	Number of high order 1s used to form a mask that is ANDed with group address ranges of candidate RPs to form a hash value. The mask determines the number of consecutive addresses to assign across RPs with the same group range. For PIM, this value ranges from 0 to 32 and has a default of 30. For PIM6, this value ranges from 0 to 128 and has a default of 126.
priority	Priority assigned to this BSR. The software elects the BSR with the highest priority, or if the BSR priorities match, the software elects the BSR with the highest IP address. This value ranges from 0, the lowest priority, to 255 and has a default of 64.

You can configure a candidate RP with the arguments and keywords described on this Table.

Table 4: BSR Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the BSR source IP address used in Bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP specified in a prefix format.
interval	Number of seconds between sending candidate-RP messages. This value ranges from 1 to 65,535 and has a default of 60 seconds. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
priority	Priority assigned to this RP. The software elects the RP with the highest priority for a range of groups, or if the priorities match, the highest IP address. (The highest priority is the lowest numerical value.) This value ranges from 0, the highest priority, to 255 and has a default of 192. **Note** This priority differs from the BSR BSR-candidate priority, which prefers the highest value between 0 and 255.
bidir	Unless you specify bidir, this RP will be in ASM mode. If you specify bidir, the RP will be in Bidir mode.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is applied.

Tip You should choose the candidate BSRs and candidate RPs that have good connectivity to all parts of the PIM domain.

You can configure the same router to be both a BSR and a candidate RP. In a domain with many routers, you can select multiple candidate BSRs and RPs to automatically fail over to alternates if a BSR or an RP fails.

To configure candidate BSRs and RPs, follow these steps:

1. Configure whether each router in the PIM domain should listen to and forward BSR messages. A router configured as either a candidate RP or a candidate BSR automatically listens to and forwards all bootstrap router protocol messages, unless an interface is configured with the domain border feature. For more information, see the *Configuring PIM or PIM6 Sparse Mode*.
2. Select the routers to act as candidate BSRs and RPs.
3. Configure each candidate BSR and candidate RP as described in this section.
4. Configure BSR message filtering. See *Configuring Message Filtering*.

Configuring BSRs (PIM)

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim bsr listen forward** *listen|forward | forward|listen* **Example:** `switch(config)# ip pim bsr listen forward`	Configures listen and forward. Ensure that you have entered this command in each VRF on the remote PE.
Step 3	**ip pim bsr**[**bsr-candidate**] *interface* [**hash-len** *hash-length*] [**priorty** *priority]* **Example:** `switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24`	Configures a candidate bootstrap router (BSR). The source IP address used in a bootstrap message is the IP address of the interface. The hash length ranges from 0 to 32 and has a default of 30. The priority ranges from 0 to 255 and has a default of 64.
Step 4	**ip pim sparse-mode** **Example:** `switch(config)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 5	**ip** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* **bidir**	(Optional) Specifies the number of Bidir RPs that you can configure for IPv6. The maximum number of Bidir RPs supported per VRF for

	Command or Action	Purpose

	Example:
	`switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24`
	Example:
	`switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir`
		PIM and PIM6 combined cannot exceed 8. Values range from 0 to 8. The default is 2.
		Configures a candidate RP for BSR. The priority ranges from 0, the highest priority, to 65,535 and has a default of 192. The interval ranges from 1 to 65,535 seconds and has a default of 60.
		Note We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
		Example 1 configures an ASM candidate RP.
		Example 2 configures a Bidir candidate RP.

Step 6	**show ip pim group-range** *ip-prefix* **vrf** *vrf-name* **all** **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM modes and group ranges.
Step 7	**ipv6 routing multicast holddown** *holddown-period* **Example:** `switch(config)# ipv6 routing multicast holddown 100`	(Optional) Saves configuration changes.

Configuring BSRs (PIM6)

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim [bsr] bsr-candidate** | *interface* [**hash-len** *hash-length* **priority** *priority]* **Example:** `switch(config)# ipv6 pim bsr-candidate ethernet 2/1 hash-len 24 priority 192`	Configures a candidate bootstrap router (BSR). The source IP address used in a bootstrap message is the IP address of the interface. The hash length ranges from 0 to 128 and has a default of 126. The priority ranges from 0, the lowest priority, to 255 and has a default of 64.
Step 3	**ipv6** [**bsr**] **rp-candidate** *interface* **group-list** *ipv6-prefix* [**route-map** *policy-name]* **priority** *priority* **interval** *interval* **bidir**]	Configures a candidate RP for BSR. The priority ranges from 0, the highest priority, to 65,535 and has a default of 192. The interval

	Command or Action	Purpose

	Example:
	`switch(config)# ipv6 pim rp-candidate ethernet 2/1 group-list ff1e:abcd:def1::0/24`
	Example:
	`switch(config)# ipv6 pim rp-candidate ethernet 2/1 group-list ff1e:abcd:def2::0/24 bidir`
		ranges from 1 to 65,535 seconds and has a default of 60.
		Example 1 configures an ASM candidate RP.
		Example 2 configures a Bidir candidate RP.

Step 4	**show ipv6 pim group-range** *ipv6-prefix* **vrf** *vrf-name* **all** **Example:** `switch(config)# show ipv6 pim group-range`	(Optional) Displays PIM6 modes and group ranges.
Step 5	**copy running-config startup-config** *holddown-period* **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Auto-RP

You can configure Auto-RP by selecting candidate mapping agents and RPs. You can configure the same router to be both a mapping agent and a candidate RP.

Note Auto-RP is not supported by PIM6.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

You can configure an Auto-RP mapping agent with the arguments described on this Table.

Table 5: Auto-RP Mapping Agent Arguments

Argument	Description
interface	Interface type and number used to derive the IP address of the Auto-RP mapping agent used in bootstrap messages.
scope *ttl*	Time-To-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32. **Note** See the border domain feature in the *Configuring PIM or PIM6 Sparse Mode*.

If you configure multiple Auto-RP mapping agents, only one is elected as the mapping agent for the domain. The elected mapping agent ensures that all candidate RP messages are sent out. All mapping agents receive the candidate RP messages and advertise the same RP cache in their RP-discovery messages.

You can configure a candidate RP with the arguments and keywords described on this Table.

Table 6: Auto-RP Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the IP address of the candidate RP used in Bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP. It is specified in a prefix format.
scope *ttl*	Time-To-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32. **Note** See the border domain feature in the *Configuring PIM or PIM6 Sparse Mode*.
interval	Number of seconds between sending RP-Announce messages. This value can range from 1 to 65,535 and has a default of 60. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
bidir	If not specified, this RP will be in ASM mode. If specified, this RP will be in Bidir mode.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is applied.

Tip You should choose mapping agents and candidate RPs that have good connectivity to all parts of the PIM domain.

To configure Auto-RP mapping agents and candidate RPs, follow these steps:

1. For each router in the PIM domain, configure whether that router should listen and forward Auto-RP messages. A router configured as either a candidate RP or an Auto-RP mapping agent will automatically listen to and forward all Auto-RP protocol messages, unless an interface is configured with the domain border feature. For more information, see the *Configuring PIM or PIM6 Sparse Mode*.
2. Select the routers to act as mapping agents and candidate RPs.
3. Configure each mapping agent and candidate RP as described in this section.

4. Configure Auto-RP message filtering. See *Configuring Message Filtering*.

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

Configuring Auto RP (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim** {**send-rp-discovery** | { **auto-rp mapping-agent** }} *interface* [**scope** *ttl*] **Example:** `sswitch(config)# ip pim auto-rp mapping-agent ethernet 2/1`	Configures an Auto-RP mapping agent. The source IP address used in Auto-RP Discovery messages is the IP address of the interface. The default scope is 32.

Step 3	**ip pim** { |**send-rp-announce** | {**auto-rp rp-candidate**]}**auto***interface* {**group-list** *ip-prefix* | **route_map** *policy-name*} [**scope** *ttl*] **interval** *interval*] [**bidir**
	Example:
	`switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24`
	Example:
	`switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir`
		Configures an Auto-RP candidate RP. The default scope is 32. The default interval is 60 seconds. By default, the command creates an ASM candidate RP. For parameter details, see Table 4-8.
		Note We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
		Example1 configures an ASM candidate RP.
		Example 2 configures a Bidir candidate RP.

Step 4	**ip pim sparse-mode** **Example:** `switch(config)# ip pim sparse-mode`	Enables PIM sparse mode on the interface. The default is disabled.
Step 5	**show ip pim group-range** *lip-prefix*] **vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM modes and group ranges.
Step 6	**copy running-config startup-config** *rate* **Example:**	(Optional) Saves configuration changes.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Configuring a PIM Anycast-RP Set

To configure a PIM Anycast-RP set, follow these steps:

1. Select the routers in the PIM Anycast-RP set.
2. Select an IP address for the PIM Anycast-RP set.
3. Configure each peer RP in the PIM Anycast-RP set as described in this section.

Configuring a PIM Anycast RP Set (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface loopback** *number* **Example:** `switch(config)# interface loopback 0`	Configures an interface loopback. This example configures interface loopback 0.
Step 3	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 192.0.2.3/32`	Configures an IP address for this interface. This example configures an IP address for the Anycast-RP.
Step 4	**ip pim sparse-mode**	Enables PIM.
Step 5	**exit** **Example:** `switch(config)# exit`	Returns to configuration mode.
Step 6	**ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* **Example:** `switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31`	Configures a PIM Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.

	Command or Action	Purpose
Step 7	Repeat Step 5 using the same Anycast-RP-address for each RP in the RP set (including the local router).	--
Step 8	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	Configures a PIM Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 9	**copy running-config startup-config** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring a PIM Anycast RP Set (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface loopback** *number* **Example:** `switch(config)# interface loopback 0`	Configures an interface loopback. This example configures interface loopback 0.
Step 3	**ipv6 address** *ipv6-prefix* **Example:** `switch(config-if)# ipv6 address 2001:0db8:0:abcd::3/32`	Configures an IP address for this interface. This example configures an IP address for the Anycast-RP.
Step 4	**ip pim sparse-mode**	Enables PIM.
Step 5	**exit** **Example:** `switch(config)# exit`	Returns to configuration mode.
Step 6	**ipv6 pim anycast-rp** *anycast-rp-address anycast-rp-peer-address*	Configures a PIM6 Anycast-RP peer address for the specified Anycast-RP address. Each

	Command or Action	Purpose
	Example: `switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::3 2001:0db8:0:abcd::31`	command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 7	Repeat Step 5 using the same Anycast-RP-address for each RP in the RP set (including the local router).	--
Step 8	**show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ipv6 pim group-range`	(Optional) Displays PIM6 modes and group ranges.
Step 9	**copy running-config startup-config** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Shared Trees Only for ASM

You can configure shared trees only on the last-hop router for Any Source Multicast (ASM) groups, which means that the router never switches over from the shared tree to the SPT when a receiver joins an active group. You can specify a group range where the use of shared trees is to be enforced with the **match ip**[**v6**] **multicast** command. This option does not affect the normal operation of the router when a source tree join-prune message is received.

Note The Cisco NX-OS software does not support the shared-tree feature on vPCs. For more information about vPCs, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*

The default is disabled, which means that the software can switch over to source trees.

Note In ASM mode, only the last-hop router switches from the shared tree to the SPT.

Configuring Shared Trees Only for ASM (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim use-shared-tree-only group-list** *policy-name* **Example:** `switch(config)# ip pim use-shared-tree-only group-list my_group_policy`	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ip multicast** command. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.
Step 3	**show ip pim group-range** [*ip-prefix*] **vrf** *vrf-name* | **all** **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM modes and group ranges.
Step 4	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Shared Trees Only for ASM (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled for PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ipv6 pim use-shared-tree-only group-list** *policy-name* **Example:** `switch(config)# ipv6 pim use-shared-tree-only group-list my_group_policy`	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ipv6 multicast command**. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.

	Command or Action	Purpose
Step 3	**show ipv6 pim group-range** [*ip-prefix*] **vrf** *vrf-name* | **all** **Example:** `switch(config)# show ipv6 pim group-range`	(Optional) Displays PIM6 modes and group ranges.
Step 4	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring SSM

Source-Specific Multicast (SSM) is a multicast distribution mode where the software on the DR connected to a receiver that is requesting data for a multicast source builds a shortest path tree (SPT) to that source.

On an IPv4 network, a host can request multicast data for a specific source only if it is running IGMPv3 and the DR for that host is running IGMPv3. You will usually enable IGMPv3 when you configure an interface for PIM in the SSM mode. For hosts running IGMPv1 or IGMPv2, you can configure a group to source mapping using SSM translation. For more information, see *Configuring IGMP* and *Configuring MLD*.

You can configure the group range that is used by SSM by specifying values on the command line. By default, the SSM group range for PIM is 232.0.0.0/8 and for PIM6 is FF3x/96.

You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command.

Note If you want to use the default SSM group range, you do not need to configure the SSM group range.

Configuring SSM (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**[no] ip pim ssm range** { *ip-prefix* | **none** | **route-map***policy-name* } **Example:**	Configures up to four group ranges to be treated in SSM mode. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The

	Command or Action	Purpose

	`switch(config)# ip pim ssm range 239.128.1.0/24`
	Example:
	`switch(config)# no ip pim ssm range none`
		default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed.
		The **no** option removes the specified prefix from the SSM range, or removes the route-map policy. If the keyword **none** is specified, resets the SSM range to the default of 232.0.0.0/8.

Step 3	**show ip pim group-range** [*ip-prefix*] **vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM mode and group ranges.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring SSM (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**[no] ipv6 pim ssm** range { *ipv6-prefix* | **none** | **route-map** *policy-name* }
	Example:
	`switch(config)# ipv6 pim ssm range FF30::0/32`
		Configures up to four group ranges to be treated in SSM mode. You can specify a route-map policy name that lists the group prefixes to use with the match ip multicast command. If the keyword none is specified, all group ranges are removed. The default range is FF3x/96.

Step 3	**show ipv6 pim group-range** [*ipv6-prefix*] **vrf***vrf-name* | **all**]	(Optional) Displays PIM6 modes and group ranges.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring RPF Routes for Multicast

You can define RPF routes for multicast when you want multicast data to diverge from the unicast traffic path. You can define RPF routes for multicast on border routers to enable reverse path forwarding (RPF) to an external network.

Multicast routes are used not to directly forward traffic but to make RPF checks. RPF routes for multicast cannot be redistributed.

Note IPv6 static multicast routes are not supported.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip mroute**{*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* | *interface*} [*route-preference*] [**vrf** *vrf-name*]
	Example:
	`switch(config)# ip mroute 192.0.2.33/1`
	`224.0.0.0/1`
		Configures an RPF route for multicast for use in RPF calculations. Route preference values range from 1 to 255. The default preference is 1.

Step 3	**show ip static-route** [**multicast**] [**vrf** *vrf-name*]
	Example:
	`switch(config)# show ip static-route`
	`multicast`
		(Optional) Displays configured static routes.

Step 4	**copy running-config startup-config** [*ip-prefix*] **vrf***vrf-name* | **all**	(Optional) Saves configuration changes.

Disabling Multicast Multipath

By default, the RPF interface for multicast is chosen automatically when there are multiple ECMP paths available. Disabling the automatic selection allows you to specify a single RPF interface for multicast.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip multicast multipath none** **Example:** `switch(config)# ip multicast multipath none`	Disables multicast multipath.
Step 3	**clear ip mroute * vrf** *vrf-name* **Example:** `switch(config)# clear ip mroute *`	Clears multipath routes and activates multicast multipath suppression.

Enabling ECMP Multicast Load Splitting Based on Source Group and Next-Hop Address

Perform this task to enable ECMP multicast load splitting of multicast traffic based on source, group, and next-hop address (using the next-hop-based S-G-hash algorithm) to take advantage of multiple paths through the network. The next-hop-based S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. Unlike the S-hash and basic S-G-hash algorithms, the hash mechanism used by the next-hop-based S-G-hash algorithm is not subject to polarization.

The next-hop-based S-G-hash algorithm provides more flexible support for ECMP multicast load splitting than S-hash algorithm and eliminates the polarization problem. Using the next-hop-based S-G-hash algorithm for ECMP multicast load splitting enables multicast traffic from devices that send many streams to groups or that broadcast many channels, such as IPTV servers or MPEG video servers, to be more effectively load split across equal-cost paths.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	**ip multicast multipath s-g-hash next-hop-based** **Example:** `switch(config)# ip multicast multipath s-g-hash next-hop-based`	Enables ECMP multicast load splitting based on source, group, and next-hop-address using the next-hop-based S-G-hash algorithm. • Because this command changes the way an RPF neighbor is selected, it must be configured consistently on all routers in a redundant topology to avoid looping.

	Command or Action	Purpose
		Note Be sure to enable the **ip multicast multipath** command on the router that is supposed to be the receiver for traffic from more than one incoming interfaces, which is opposite to unicast routing. From the perspective of unicast, multicast is active on the sending router connecting to more than one outgoing interfaces.
Step 3	Repeat Steps 1 through 3 on all the routers in a redundant topology.	--

Step 4	**end**
	Example:
	`switch(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Step 5	**show ip rpf** *source-address* [*group-address*] **Example:** `switch# show ip rpf 10.1.1.2`	(Optional) Displays the information that IP multicast routing uses to perform the RPF check. • Use this command to verify RPF selection so as to ensure that IP multicast traffic is being properly load split.
Step 6	**show ip route** *ip-address* **Example:** `switch# show ip route 10.1.1.2`	(Optional) Displays the current state of the IP routing table. • Use this command to verify that there multiple paths available to a source or RP for ECMP multicast load splitting. • For the *ip-address* argument, enter the IP address of a source to validate that there are multiple paths available to the source (for shortest path trees) or the IP address of an RP to validate that there are multiple paths available to the RP (for shared trees).

Example: Enabling ECMP Multicast Load Splitting Based on Source Group and Next-Hop Address

The following example shows how to enable ECMP multicast load splitting on a router based on source, group, and next-hop address using the next-hop-based S-G-hash algorithm:

```
switch(config)# ip multicast multipath s-g-hash next-hop-based
```

Configuring Route Maps to Control RP Information Distribution

You can configure route maps to help protect against some RP configuration errors and malicious attacks. You use route maps in commands that are described in the *Configuring Message Filtering*.

By configuring route maps, you can control distribution of RP information that is distributed throughout the network. You specify the BSRs or mapping agents to be listened to on each client router and the list of candidate RPs to be advertised (listened to) on each BSR and mapping agent to ensure that what is advertised is what you expect.

See the *Configuring BSRs* and *Configuring Auto-RP* for more information.

Note Only the **match ipv6 multicast** command has an effect in the route map.

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

Configuring Route Maps to Control RP Information Distribution (PIM)

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**route-map** *map-name* | **permit** | **deny**] [*sequence-number*]
	Example:
	`switch(config)# route-map ASM_only permit 10`
	`switch(config-route-map)#`
	Example:
	`switch(config)# route-map Bidir_only permit 10`
	`switch(config-route-map)#`
		Enters route-map configuration mode.
		Note This configuration method uses the **permit** keyword.

Step 3	**match ip multicast** {{**rp** *ip-address* [**rp-type** *rp-type*]} {{**group-range** {*gadrr_start* **to** *gadrr_end*} | {*group ip-prefix*}} {**source** *source-ip-address*}
	Example:
	`switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`
	Example:
		Matches the group, RP, and RP type specified. You can specify the RP type (ASM or Bidir). This configuration method requires the group and RP specified as shown in the examples.
		Note BSR RP, auto-RP, and static RP cannot use the **group-range** keyword. This command allows both permit or deny. Some match mask commands do not allow permit or deny.

	Command or Action	Purpose
	`switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bdir`	
Step 4	**show route-map** **Example:** `switch(config-route-map)# show route-map`	(Optional) Displays configured route maps.
Step 5	**copy running-config startup-config** **Example:** `switch(config-route-map)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Route Maps to Control RP Information Distribution (PIM6)

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**route-map** *map-name* [**permit**| **deny**] [*sequence-number*]
	Example:
	`switch(config)# route-map ASM_only permit 10`
	`switch(config-route-map)#`
	Example:
	`switch(config)# route-map Bidir_only permit 10`
	`switch(config-route-map)#`
		Enters route-map configuration mode.
		Note This configuration method uses the **permit** keyword.

Step 3	**match ipv6 multicast** {{**rp** *ip-address* [**rp-type** *rp-type*]} {{**group-range** {*gadrr_start* **to** *gadrr_end*} | {*group ip-prefix*}} {**source** *source-ip-address*}
	Example:
	`switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`
	Example:
	`switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bdir`
		Matches the group, RP, and RP type specified. You can specify the RP type (ASM or Bidir). This configuration method requires the group and RP specified as shown in the examples.
		Note BSR RP, auto-RP, and static RP cannot use the **group-range** keyword. This command allows both permit or deny. Some match mask commands do not allow permit or deny.

	Command or Action	Purpose
Step 4	**show route-map** **Example:** `switch(config-route-map)# show route-map`	(Optional) Displays configured route maps.

Step 5	**copy running-config startup-config**
	Example:
	`switch(config-route-map)# copy`
	`running-config startup-config`
		(Optional) Saves configuration changes.

Configuring Message Filtering

Note Prefix matches in the rp-candidate-policy must be exact relative to what the c-rp is advertising. Subset matches are not possible.

You can configure filtering of the PIM and PIM6 messages described in the table below.

Table 7: PIM and PIM6 Message Filtering

Message Type	Description
Global to the Device	
Log Neighbor changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
PIM register policy	Enables PIM register messages to be filtered based on a route-map policy[2] where you can specify group or group and source addresses with the **match ip[v6] multicast** command. This policy applies to routers that act as an RP. The default is disabled, which means that the software does not filter PIM register messages.
BSR candidate RP policy	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy1 where you can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ip[v6] multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.
BSR policy	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy1 where you can specify BSR source addresses with the **match ip[v6] multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.

Message Type	Description
Auto-RP candidate RP policy	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy1 where you can specify the RP and group addresses, and whether the type is Bidir or ASM with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages. **Note** PIM6 does not support the Auto-RP method.
Auto-RP mapping agent policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy1 where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages. **Note** PIM6 does not support the Auto-RP method.
Per Device Interface	
Join-prune policy	Enables join-prune messages to be filtered based on a route-map policy1 where you can specify group, group and source, or group and RP addresses with the **match ip[v6] multicast** command. The default is no filtering of join-prune messages.

[2] For information about configuring route-map policies, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Route maps as a filtering policy can be used (either **permit** or **deny** for each statement) for the following commands:

- **jp-policy** can use (S,G), (*,G), or (RP,G)
- **register-policy** can use (S,G) or (*,G)
- **igmp report-policy** can use (*,G) or (S,G)
- **state-limit reserver-policy** can use (*,G) or (S,G)
- **auto-rp rp-candidate-policy** can use (RP,G)
- **bsr rp-candidate-policy** can use (group-range/G, RP, RP-type)
- **autorp mapping-agent policy** can use (S)
- **bsr bsr-policy** can use (S)

Route maps as containers can be use for the following commands, where route-map action (**permit** or **deny**) is ignored:

- **ip pim rp-address route map** can use only G
- **ip pim ssm-range route map** can use only G
- **ip igmp static-oif route map** can use (S,G), (*,G), (S,G-range), (*,G-range)
- **ip igmp join-group route map** can use (S,G), (*,G), (S,G-range, (*, G-range)

Configuring Message Filtering (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled for PIM.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim log-neighbor-changes**
	Example:
	`switch(config)# ip pim`
	`log-neighbor-changes`
		(Optional) Enables syslog messages that list the neighbor state changes to be generated. The default is disabled..

Step 3	**ip pim register-policy** *policy-name*
	Example:
	`switch(config)# ip pim register-policy`
	` my_register_policy`
		(Optional) Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ip multicast** command.

Step 4	**ip pim bsr rp-candidate-policy** *policy-name*
	Example:
	`switch(config)# ip pim bsr`
	`rp-candidate-policy`
	`my_bsr_rp_candidate_policy`
		(Optional) Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.

Step 5	**ip pim bsr bsr-policy** *policy-name*
	Example:
	`switch(config)# ip pim bsr bsr-policy`
	`my_bsr_policy`
		(Optional) Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.

	Command or Action	Purpose
Step 6	**ip pim auto-rp rp-candidate-policy** *policy-name* **Example:** `switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy`	(Optional) Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages.
Step 7	**ip pim auto-rp mapping-agent-policy** *policy-name* **Example:** `switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy`	(Optional) Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages.

Step 8	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 9	**ip pim jp-policy** *policy-name*[in | out] **Example:** `switch(config-if)# ip pim jp-policy my_jp_policy`	(Optional) Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the**match ip multicast** command. The default is no filtering of join-prune messages. Beginning with Cisco NX-OS Release 4.2(3), this command filters messages in both incoming and outgoing directions.
Step 10	**show run pim** **Example:** `switch(config-if)# show run pim`	(Optional) Displays PIM configuration commands.
Step 11	**copy running-config startup-config** *interval* **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Message Filtering (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled for PIM6.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ipv6 pim log-neighbor-changes**
	Example:
	`switch(config)# ipv6 pim`
	`log-neighbor-changes`
		(Optional) Enables syslog messages that list the neighbor state changes to be generated. The default is disabled..

Step 3	**ipv6 pim register-policy** *policy-name*
	Example:
	`switch(config)# ipv6 pim register-policy`
	` my_register_policy`
		(Optional) Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ipv6 multicast** command. The default is disabled.

Step 4	**ipv6 pim bsr rp-candidate-policy** *policy-name*
	Example:
	`switch(config)# ipv6 pim bsr`
	`rp-candidate-policy`
	`my_bsr_rp_candidate_policy`
		(Optional) Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ipv6 multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.

Step 5	**ipv6 pim bsr bsr-policy** *policy-name*
	Example:
	`switch(config)# ipv6 pim bsr bsr-policy`
	` my_bsr_policy`
		(Optional) Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ipv6 multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.

Step 6	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 7	**ipv6 pim jp-policy** *policy-name*[**in** | **out**]
	Example:
	`switch(config-if)# ipv6 pim jp-policy`
	`my_jp_policy`
		(Optional) Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the**match ipv6 multicast** command. The default is no filtering of join-prune messages.
		Beginning with Cisco NX-OS Release 4.2(3), this command filters messages in both incoming and outgoing directions.

	Command or Action	Purpose
Step 8	**show run pim6** **Example:** `switch(config-if)# show run pim6`	(Optional) Displays PIM6 configuration commands.
Step 9	**copy running-config startup-config** *interval* **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Restarting the PIM and PIM6 Processes

You can restart the PIM and PIM6 processes and optionally flush all routes. By default, routes are not flushed.

When routes are flushed, they are removed from the Multicast Routing Information Base (MRIB and M6RIB) and the Multicast Forwarding Information Base (MFIB and M6FIB).

When you restart PIM or PIM6, the following tasks are performed:

- The PIM database is deleted.
- The MRIB and MFIB are unaffected and forwarding of traffic continues.
- The multicast route ownership is verified through the MRIB.
- Periodic PIM join and prune messages from neighbors are used to repopulate the database.

Restarting the PIM Process (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose
Step 1	**restart pim** **Example:** `switch# restart pim`	Restarts the PIM process.

Step 2	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**ip pim flush-routes** **Example:** `switch(config)# ip pim flush-routes`	Removes routes when the PIM process is restarted. By default, routes are not flushed.

	Command or Action	Purpose
Step 4	**show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	(Optional) Displays the PIM running-configuration information, including the flush-routes command.
Step 5	**copy running-config startup-config** *policy-name* **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Restarting the PIM6 Process

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

Procedure

	Command or Action	Purpose
Step 1	**restart pim6** **Example:** `switch# restart pim`	Restarts the PIM process.

Step 2	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**ipv6 pim flush-routes** **Example:** `switch(config)# ipv6 pim flush-routes`	Removes routes when the PIM6 process is restarted. By default, routes are not flushed.
Step 4	**show running-configuration pim6** **Example:** `switch(config)# show running-configuration pim6`	(Optional) Displays the PIM6 running-configuration information, including the **flush-routes** command.
Step 5	**copy running-config startup-config** *policy-name* **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring BFD for PIM in VRF Mode

Note You can configure BFD for PIM by either VRF or by interface.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vrf context** *vrf-name*
	Example:
	`switch# vrf convrf-name`
	`text test`
	`switch(config-vrf)#`
		Enters VRF configuration mode.

Step 3	**ip pim bfd** **Example:** `switch(config-vrf)# ip pim bfd`	Enables BFD on the specified VRFs. **Note** You can also enter the **ip pim bfd** command in configuration mode, which enables BFD on VRF. Enters VRF configuration mode.

Configuring BFD for PIM in Interface Mode

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch(config)# interface ethernet 7/40`
	`switch(config-if)#`
		Enters global configuration mode.

Step 2	**interface** *interface-type*
	Example:
	`switch(config)# interface ethernet 7/40`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	**config tip pim bfd instance** **Example:** `switch(config-if)# ip pim bfd instance`	Enables BFD on the specified interfaces. You can enable or disable BFD on RIM interfaces irrespective of whether BFD is enabled on the VRF.

	Command or Action	Purpose
Step 4	**exit** **Example:** `switch(config)# exit`	Exits out of VRF or interface configuration mode.
Step 5	**show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	(Optional) Displays the PIM running-configuration information.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Verifying the PIM and PIM6 Configuration

To display the PIM and PIM6 configurations information, perform one of the following tasks. Use the **show ip** form of the command for PIM and the **show ipv6** form of the command for PIM6.

Command	Description
show ip [**v6**] **mroute** {*source group* | *group* [*source*]} [**vrf** *vrf-name* | **all**]	Displays the IP or IPv6 multicast routing table.
show ip [**v6**] **pim df** [**vrf** *vrf-name* | **all**]	Displays the designated forwarder (DF) information for each RP by interface.
show ip [**v6**] **pim group-range** [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see also the **show ip pim rp** command.
show ip [**v6**] **pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays information by the interface.
show ip [**v6**] **pim neighbor** [**vrf** *vrf-name* | **all**]	Displays neighbors by the interface.
show ip [**v6**] **pim oif-list** *group* [*source*] [**vrf** *vrf-name* | **all**]	Displays all the interfaces in the OIF-list.
show ip [**v6**] **pim route** {source group | group [source]} [**vrf** *vrf-name* | **all**]	Displays information for each multicast route, including interfaces on which a PIM join for that (S, G) has been received.
show ip [**v6**] **pim rp** [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known to the software, how they were learned, and their group ranges. For similar information, see also the **show ip pim group-range** command.

Command	Description
show ip [**v6**] **pim rp-hash** [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information. For information about the RP hash, see *RFC 5059*.
show running-configuration pim[**6**]	Displays the running-configuration information.
show startup-configuration pim[**6**]	Displays the startup-configuration information.
show ip [**v6**] **pim vrf** [*vrf-name* **| all]** [**detail**]	Displays per-VRF information.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*.

Displaying Statistics

You can display and clear PIM and PIM6 statistics by using the commands in this section.

Displaying PIM and PIM6 Statistics

You can display the PIM and PIM6 statistics and memory usage using the commands listed in the table below. Use the **show ip** form of the command for PIM and the **show ipv6** form of the command for PIM6.

Command	Description
show ip [v6] pim policy statistics	Displays policy statistics for Register, RP, and join-prune message policies.
show ip [v6] pim statistics [**vrf** *vrf-name* | **all**]	Displays global statistics. If PIM is in vPC mode, displays vPC statistics.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*.

Clearing PIM and PIM6 Statistics

You can clear the PIM and PIM6 statistics using the commands listed in the table below. Use the **show ip** form of the command for PIM and the **show ipv6** form of the command for PIM6.

Command	Description
ip [v6] pim interface statistics*interface*	Clears counters for the specified interface.
clear ip [v6] pim policy statistics	Clears policy counters for Register, RP, and join-prune message policies.
clear ip [v6] pim statistics [**vrf-name** | **all**]	Clears global counters handled by the PIM process.

Command	Description
clear ip mroute statistics {***** | *ipv4-grp-addr/prefix-length*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]	Clears software and hardware statistics for all or specific multicast routes or multicast prefixes. **Note** Use the **show ip mroute** command to display the statistics for multicast route and prefixes.

Displaying Replication Engine Statistics

You can display replication engine statistics by using the **show hardware replication-engine statistics** [*module mod-no*] [*instance inst-no*] command.

Replication Engine Statistics Example

```
switch# show hard rep stat mod 10 inst 0
Replication Engine Statistics for Module 10 (N7K-M108X2-12L)

Instance 0 (ports 1-2):
Packet Counters:
Description                                  InPkts            OutPkts
-----------------------------------------------------------------------
Interface In Hi (port 1)                          0                  0
Interface In Lo (port 1)                          0                  0
Interface In Hi (port 2)                          0                  0
Interface In Lo (port 2)                          0                  0
Interface Out Hi (port 1)                         0                  0
Interface Out Lo (port 1)                         0                  0
Interface Out Hi (port 2)                         0                  0
Interface Out Lo (port 2)                         0                  0
Fabric In Hi                                      0                  0
Fabric In Lo                                      0                  0
Fabric Out Hi                                     0                  0
Fabric Out Lo                                     0                  0
Fwding Engine Tx                                  0                  0
Fwding Engine Rx                                  0                  0
Fwding Engine Ucast Rx                            0                  0
Fwding Engine Mcast Rx                            0                  0
Fwding Engine Rx                                  0                  0
Replication In Ucast                              0                  0
Replication Out Ucast                             0                  0
Replication In Mcast                              0                  0
Replication Out Mcast                             0                  0

Rates:
Description                         In PPS       In Bps       Out PPS      Out Bps
-----------------------------------------------------------------------------------
Interface In Hi (port 1)                 0            0             0            0
Interface In Lo (port 1)                 0            0             0            0
Interface In Hi (port 2)                 0            0             0            0
Interface In Lo (port 2)                 0            0             0            0
Interface Out Hi (port 1)                0            0             0            0
Interface Out Lo (port 1)                0            0             0            0
Interface Out Hi (port 2)                0            0             0            0
Interface Out Lo (port 2)                0            0             0            0
Fabric In Hi                             0            0             0            0
Fabric In Lo                             0            0             0            0
Fabric Out Hi                            0            0             0            0
Fabric Out Lo                            0            0             0            0
Fwding Engine Tx                         0            0             0            0
Fwding Engine Rx                         0            0             0            0
Fwding Engine Ucast Rx                   0            0             0            0
Fwding Engine Mcast Rx                   0            0             0            0
Fwding Engine Rx                         0            0             0            0
Replication In Ucast                     0            0             0            0
Replication Out Ucast                    0            0             0            0
Replication In Mcast                     0            0             0            0
Replication Out Mcast                    0            0             0            0


Drop Counters:
Description                                  Drops
---------------------------------------------------
Multicast/SPAN FIFO Drops                        0
SPAN Rate Limiter Drops                          0

SPAN Rate Limiter State: DISABLED

Peak Rates:
Packets per second:
Description                  Peak PPS            Date/Time
------------------------------------------------------------
Interface In (port 1)               0      yyyy/mm/dd hh:ss
Interface In (port 2)               0      yyyy/mm/dd hh:ss
Interface Out (port 1)              0      yyyy/mm/dd hh:ss
Interface Out (port 2)              0      yyyy/mm/dd hh:ss
Fabric In                           0      yyyy/mm/dd hh:ss
Fabric Out                          0      yyyy/mm/dd hh:ss
Replication In Ucast                0      yyyy/mm/dd hh:ss
Replication Out Ucast               0      yyyy/mm/dd hh:ss
Replication In Mcast                0      yyyy/mm/dd hh:ss
Replication Out Mcast               0      yyyy/mm/dd hh:ss

Bytes per second:
Description                  Peak Bps            Date/Time
------------------------------------------------------------
Interface In (port 1)               0      yyyy/mm/dd hh:ss
Interface In (port 2)               0      yyyy/mm/dd hh:ss
Interface Out (port 1)              0      yyyy/mm/dd hh:ss
Interface Out (port 2)              0      yyyy/mm/dd hh:ss
Fabric In                           0      yyyy/mm/dd hh:ss
Fabric Out                          0      yyyy/mm/dd hh:ss

switch#
```

Configuration Examples for PIM

Note See the *Multiple RPs Configured in a PIM Domain* for more configuration examples.

This section describes how to configure PIM using different data distribution modes and RP selection methods.

SSM Configuration Example

To configure PIM in SSM mode, follow these steps for each router in the PIM domain:

1. Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2. Configure the parameters for IGMP that support SSM. See *Configuring IGMP* Usually, you configure IGMPv3 on PIM interfaces to support SSM.

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip igmp version 3
```

3. Configure the SSM range if you do not want to use the default range.

```
switch# config t
switch(config)# ip pim ssm range 239.128.1.0/24
```

4. Configure message filtering.

```
switch# config t
switch(config)# ip pim log-neighbor-changes
```

The following example shows how to configure PIM SSM mode:

```
config t
  interface ethernet 2/1
    ip pim sparse-mode
    ip igmp version 3
    exit
  ip pim ssm range 239.128.1.0/24
  ip pim log-neighbor-changes
```

BSR Configuration Example

To configure PIM in ASM mode using the BSR mechanism, follow these steps for each router in the PIM domain:

1. Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2. Configure whether that router should listen and forward BSR messages

```
switch# config t
switch(config)# ip pim bsr forward listen
```

3. Configure the BSR parameters for each router that you want to act as a BSR.

   ```
   switch# config t
   switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 30
   ```

4. Configure the RP parameters for each router that you want to act as a candidate RP

   ```
   switch# config t
   switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
   ```

5. Configure message filtering.

   ```
   switch# config t
   switch(config)# ip pim log-neighbor-changes
   ```

This example shows how to configure PIM ASM mode using the BSR mechanism and how to configure the BSR and RP on the same router:

```
config t
  interface ethernet 2/1
    ip pim sparse-mode
    exit
  ip pim bsr forward listen
ip pim bsr-candidate ethernet 2/1 hash-len 30
  ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
  ip pim log-neighbor-changes
```

Auto-RP Configuration Example

To configure PIM in Bidir mode using the Auto-RP mechanism, follow these steps for each router in the PIM domain:

1. Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

   ```
   switch# config t
   switch(config)# interface ethernet 2/1
   switch(config-if)# ip pim sparse-mode
   ```

2. Configure whether that router should listen and forward Auto-RP messages.

   ```
   switch# config t
   switch(config)# ip pim auto-rp forward listen
   ```

3. Configure the mapping agent parameters for each router that you want to act as a mapping agent.

   ```
   switch# config t
   switch(config)# ip pim auto-rp mapping-agent ethernet 2/1
   ```

4. Configure the RP parameters for each router that you want to act as a candidate RP.

   ```
   switch# config t
   switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir
   ```

5. Configure message filtering.

```
switch# config t
switch(config)# ip pim log-neighbor-changes
```

This example shows how to configure PIM Bidir mode using the Auto-RP mechanism and how to configure the mapping agent and RP on the same router:

```
config t
  interface ethernet 2/1
    ip pim sparse-mode
    exit
  ip pim auto-rp listen
  ip pim auto-rp forward
  ip pim auto-rp mapping-agent ethernet 2/1
  ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir
  ip pim log-neighbor-changes
```

PIM Anycast RP Configuration Example

To configure ASM mode using the PIM Anycast-RP method, follow these steps for each router in the PIM domain:

1. Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2. Configure the RP address that you configure on all routers in the Anycast-RP set.

```
switch# config t
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.3/32
```

3. Configure a loopback with an address to use in communication between routers in the Anycast-RP set for each router that you want to be in the Anycast-RP set.

```
switch# config t
switch(config)# interface loopback 1
switch(config-if)# ip address 192.0.2.31/32
```

4. Configure the Anycast-RP parameters and repeat with the IP address of each Anycast-RP for each router that you want to be in the Anycast-RP set. This example shows two Anycast-RPs.

```
switch# config t
switch(config)# ip pim anycast-rp 192.0.2.3 193.0.2.31
switch(config)# ip pim anycast-rp 192.0.2.3 193.0.2.32
```

5. Configure message filtering.

```
switch# config t
switch(config)# ip pim log-neighbor-changes
```

This example shows how to configure PIM ASM mode using two Anycast-RPs:

```
config t
interface ethernet 2/1
ip pim sparse-mode
exit
interface loopback 0
```

```
ip address 192.0.2.3/32
exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
ip pim log-neighbor-changes
```

Prefix-Based and Route-Map-Based Configurations

```
ip prefix-list plist11 seq 10 deny 231.129.128.0/17
ip prefix-list plist11 seq 20 deny 231.129.0.0/16
ip prefix-list plist11 seq 30 deny 231.128.0.0/9
ip prefix-list plist11 seq 40 permit 231.0.0.0/8

ip prefix-list plist22 seq 10 deny 231.129.128.0/17
ip prefix-list plist22 seq 20 deny 231.129.0.0/16
ip prefix-list plist22 seq 30 permit 231.128.0.0/9
ip prefix-list plist22 seq 40 deny 231.0.0.0/8

ip prefix-list plist33 seq 10 deny 231.129.128.0/17
ip prefix-list plist33 seq 20 permit 231.129.0.0/16
ip prefix-list plist33 seq 30 deny 231.128.0.0/9
ip prefix-list plist33 seq 40 deny 231.0.0.0/8

ip pim rp-address 21.21.0.11 prefix-list plist11
ip pim rp-address 21.21.0.22 prefix-list plist22
ip pim rp-address 21.21.0.33 prefix-list plist33
route-map rmap11 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap11 deny 20
 match ip multicast group 231.129.0.0/16
route-map rmap11 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap11 permit 40
 match ip multicast group 231.0.0.0/8

route-map rmap22 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap22 deny 20
 match ip multicast group 231.129.0.0/16
route-map rmap22 permit 30
 match ip multicast group 231.128.0.0/9
route-map rmap22 deny 40
 match ip multicast group 231.0.0.0/8

route-map rmap33 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap33 permit 20
 match ip multicast group 231.129.0.0/16
route-map rmap33 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap33 deny 40
 match ip multicast group 231.0.0.0/8

ip pim rp-address 21.21.0.11 route-map rmap11
ip pim rp-address 21.21.0.22 route-map rmap22
ip pim rp-address 21.21.0.33 route-map rmap33
```

Output

```
dc3rtg-d2(config-if)# show ip pim rp
```

```
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 21.21.0.11, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap11, group ranges:
      231.0.0.0/8  231.128.0.0/9 (deny)
      231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 21.21.0.22, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap22, group ranges:
      231.0.0.0/8 (deny) 231.128.0.0/9
      231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 21.21.0.33, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap33, group ranges:
      231.0.0.0/8 (deny) 231.128.0.0/9 (deny)
      231.129.0.0/16  231.129.128.0/17 (deny)

dc3rtg-d2(config-if)# show ip mroute
IP Multicast Routing Table for VRF "default"

(*, 231.1.1.1/32), uptime: 00:07:20, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 1.1.0.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:07:20, igmp

(*, 231.128.1.1/32), uptime: 00:14:27, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 1.1.0.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:27, igmp

(*, 231.129.1.1/32), uptime: 00:14:25, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 1.1.0.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:25, igmp

(*, 231.129.128.1/32), uptime: 00:14:26, igmp pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:26, igmp

(*, 232.0.0.0/8), uptime: 1d20h, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)

dc3rtg-d2(config-if)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
232.0.0.0/8        SSM       -                -
231.0.0.0/8        ASM       21.21.0.11       -
231.128.0.0/9      ASM       21.21.0.22       -
231.129.0.0/16     ASM       21.21.0.33       -
231.129.128.0/17   Unknown   -                -
```

Related Documents

Related Topic	Document Title
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
CLI commands	*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*
Configuring VRFs and Policy Based Routing	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for PIM and PIM6

Feature Name	Release	Feature Information
Support for Graceful Restart PIM	6.2(2)	Support for Graceful Restart protocol Independent Multicast (PIM) is a multicast high availability (HA) enhancement that improves the reconvergence of multicast routes (mroutes) after a route processor (RP) switchover. In the event of an RP switchover, this feature uses the PIM-SM Generation ID (GenID) value as a mechanism to trigger adjacent PIM neighbors on an interface to send PIM messages for all (*, G) and (S, G) mroutes that use that interface as an RPF interface, immediately reestablishing those states on the newly active RP.
Support for the **pim register-source** command.	5.2(1)	Support for configuring the IP source address of register messages.
BFD support for PIM (IPv4)	5.0(2)	BFD supported for PIM with IPv4.

Feature Name	Release	Feature Information
vPC	4.1(3)	Cisco NX-OS software for the Nexus 7000 Series devices does not support PIM SSM or BIDR on a vPC. Display vPC statistics with the **show ip pim statistics** command.