

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.

- About PIM and PIM6, on page 1
- Prerequisites for PIM and PIM6, on page 13
- Guidelines and Limitations for PIM and PIM6, on page 14
- Default Settings, on page 20
- Configuring PIM and PIM6, on page 22
- Verifying the PIM and PIM6 Configuration, on page 72
- Displaying Statistics, on page 78
- Null-Register Packing, on page 79
- Configuring Multicast Service Reflection, on page 80
- Configuration Examples for PIM, on page 93
- Tech-support Command, on page 104
- Related Documents, on page 105
- Standards, on page 105
- MIBs, on page 105

About PIM and PIM6

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.

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 rendezvous points (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.

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

In Cisco NX-OS, multicast is enabled only after you enable the PIM and 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.

You use the PIM and PIM6 global configuration parameters to configure the range of multicast group addresses to be handled by these 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.
- Source-Specific 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.



Note Cisco Nexus 9000 Series switches do not support PIM6 Bidir.

You can combine these modes to cover different ranges of group addresses.

For more information about PIM sparse mode and shared distribution trees used by the 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 RFC 5015.

PIM SSM with vPC

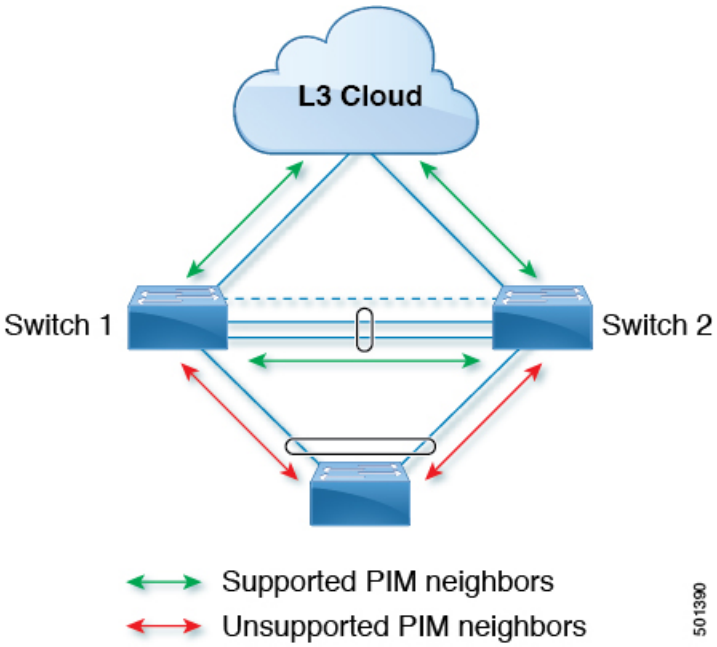
Beginning with Cisco NX-OS Release 7.0(3)I4(1), you can enable PIM SSM on Cisco Nexus 9000 Series switches with an upstream Layer 3 cloud along with the vPC feature.

A PIM adjacency between a 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.



Note Cisco Nexus 9508 switches with the N9K-X9636C-R and N9K-X9636Q-R line cards support PIM SSM beginning with Cisco NX-OS Release 7.0(3)F2(1) but do not support PIM SSM on vPCs until Cisco NX-OS Release 7.0(3)F3(1). The N9K-X9636C-RX line card supports PIM SSM with and without vPCs beginning with Cisco NX-OS Release 7.0(3)F3(1).



PIM Flooding Mechanism and Source Discovery

Protocol Independent Multicast (PIM) flooding mechanism with Source Discovery (SD) (PFM-SD) eliminates the necessity for Rendezvous Points (RPs) while sending the multicast data streams. This technique is suitable for deployments that are concerned with switch over from shared tree to shorter path (*, G) tree delays.. This technique in PIM provides a way to support PIM-Sparse Mode (SM) without the need for PIM registers, RP, or shared trees. This technique is efficient and only creates (S,G) trees. Multicast source information can be propagated throughout the multicast domain using the PIM flooding mechanism. The PFM-SD mode can coexist with the Non-Blocking Multicast (NBM). For more information about PIM-SD mode, see RFC 8364.

Beginning with Cisco NX-OS Release 10.3(2)F, the PFM-SD feature is supported for IPv4 on Cisco Nexus 9000 Series, Nexus 9800 switches, and Cisco Nexus 9504/9508 switches with N9K-X9636C-R, N9K-X9636Q-R,N9K-X9636C-RX and N9K-X96136YC-R line cards.

Hello Messages

The PIM process begins when the router establishes PIM neighbor adjacencies by sending PIM hello messages to the multicast IPv4 address 224.0.0.13 or IPv6 address ff02::d. 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.

The configured hold-time changes may not take effect on first two hellos sent after enabling or disabling PIM on an interface. For the first two hellos sent on the interface, thereafter, the configured hold times will be

used. This may cause the PIM neighbor to set the incorrect neighbor timeout value for the initial neighbor setup until a hello with the correct hold time is received.

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



Note PIM6 does not support MD5 authentication.

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 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.

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.

Due to scalability optimizations in NX-OS, it can take up to 8 minutes for an OIF entry to be deleted after Join packets for the entry are no longer received, if there is still active traffic for the group or other OIFs are still present.

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

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.

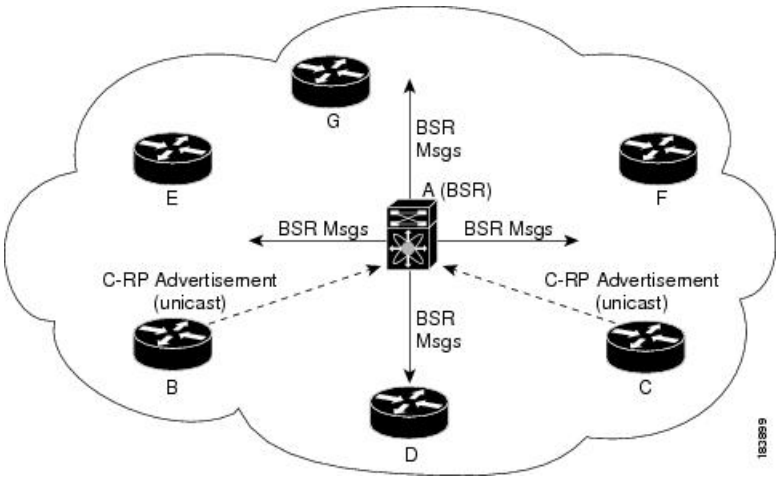
BSR is supported on Cisco Nexus 9300-FX, Cisco Nexus 9300-FX2, and Cisco Nexus 9300-FX3S platform switches.

BSR is supported on Cisco Nexus 9300-EX/FX/FX2/FX3/GX/C and 9500-EX/FX/GX platform switches.

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 might 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.

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

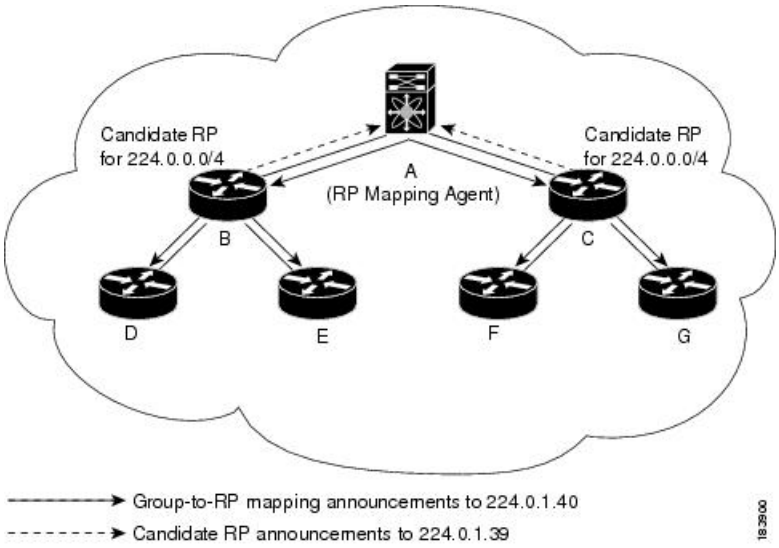
Note BSR is not supported for PIM6.

Auto-RP

Auto-RP is a Cisco protocol that was introduced 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.

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



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.

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

Multiple RPs Configured in a PIM Domain

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

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 messages will be sent in the direction of the next-closest RP.

You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidir RP.

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

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.

The PIM triggered register is enabled by default.

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.

The following 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.

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 (S, G) PIM join or prune messages toward 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.

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 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 into 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.

During the switchover, messages on the SPT and shared tree might 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.

Multicast Flow Path Visibility

Beginning with Cisco NX-OS Release 10.2(1)F, Multicast Flow Path Visualization (FPV) is supported. This feature enables you to export all multicast states in a Cisco Nexus 9000 Series switch. This helps to have a complete and reliable traceability of the flow path from the source to a receiver.

To enable Multicast Flow Path Data Export on Cisco Nexus 9000 Series switches, use the **multicast flow-path export** command.

This feature supports the following:

- Flow Path Visualization (FPV).
- Export flow statistics and states for failure detection.
- Root cause analysis on the switches along the flow path. This is done by running the appropriate debug commands.

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 on that interface.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value.

Multicast Counters

Multicast flow counters collection can be enabled in two different ways.

- Enable multicast heavy template as described in the Enabling the Multicast Heavy Template section.
- Configure the **hardware profile multicast flex-stats-enable** command in the default template.

Only Cisco Nexus 9300-EX, X9700-FX, 9300-FX, and 9300-FX2 Series switches support multicast counters. These counters provide more granularity and visibility about multicast traffic. Specifically, they show an absolute multicast packet count (bytes and rate for every multicast S,G route). These counters are valid only for S,G routes and not for *,G routes. Multicast counters appear in the output of the **show ip mroute detail**and **show ip mroute summary** commands when the multicast heavy template is enabled.

Beginning with Cisco NX-OS Release 10.6(1)F, multicast flow counter feature for IPv4 is supported on Cisco Nexus N9336C-SE1. To enable this feature, execute **hardware profile multicast flex-stats-enable** command and reload the switch using **copy running-config startup-config** command.

Beginning with Cisco NX-OS Release 10.6(2)F, multicast flow counter feature for IPv4 is supported on Cisco Nexus N9324C-SE1U, N9348Y2C6D-SE1U, N9396Y12C-SE1, and N9396T12C-SE1 switches. To enable

this feature, execute **hardware profile multicast flex-stats-enable** command and reload the switch using **copy running-config startup-config** command.

Multicast Heavy Template

You can enable the multicast heavy template in order to support significantly more multicast routes and to display multicast counters in the output of the **show ip mroute** command.

The multicast heavy template is supported for the following devices and releases:

- Cisco Nexus N9K-X9732C-EX, N9K-X9736C-E, and N9K-X97160YC-EX line cards, beginning with Cisco NX-OS Release 7.0(3)I3(2), but only for increased scalability
- Cisco Nexus 9300-EX Series switches, beginning with Cisco NX-OS Release 7.0(3)I6(1), for both increased scalability and multicast counters
- Cisco Nexus 9300-FX Series switches, beginning with Cisco NX-OS Release 7.0(3)I7(1), for both increased scalability and multicast counters

Multicast VRF-Lite Route Leaking

Beginning with Cisco NX-OS Release 7.0(3)I7(1), multicast receivers can forward IPv4 traffic across VRFs. In previous releases, multicast traffic can flow only within the same VRF.

With multicast VRF-lite route leaking, Reverse Path Forwarding (RPF) lookup for multicast routes in the receiver VRF can be performed in the source VRF. Therefore, traffic originating from the source VRF can be forwarded to the receiver VRF.

PIM Graceful Restart

Protocol Independent Multicast (PIM) graceful restart 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 PIM graceful restart 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.

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.

PIM Graceful Restart Operations

This figure illustrates the operations that occur after a route processor (RP) switchover on devices that support the PIM graceful restart feature.

Figure 3: PIM Graceful Restart Operations During an RP Switchover

The PIM graceful restart operations 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 PIM graceful restart for all (*, G) and (S, G) mroutes that use that interface as an RPF interface.
- Those mroute states are then immediately reestablished on the newly active RP.

PIM Graceful Restart and Multicast Traffic Flow

Multicast traffic flow on PIM neighbors is not affected if the multicast traffic detects support for PIM graceful restart PIM or PIM hello messages 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 might not function as per design if you configure the PIM hello interval with a value lower than the default value of 30 seconds.

High Availability

When a route processor reloads, multicast traffic across VRFs behaves the same as traffic forwarded within the same VRF.

For information about high availability, see the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*.

Prerequisites for PIM and PIM6

PIM has the following prerequisites:

PIM and PIM6 have the following prerequisites:

- You are logged onto the device.
- 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.
- For PIM Bidir, you must configure the ACL TCAM region size using the **hardware access-list tcam region mcast-bidir** command.

  Use the **hardware access-list tcam region ing-sup** command to change the ACL TCAM region size and to configure the size of the ingress supervisor TCAM region.

  See Configuring ACL TCAM Region Sizes for more information.

Note This limitation does not apply to Cisco Nexus 9300-EX Series switches.

Note By default the mcast-bidir region size is zero. You need to allocate enough entries to this region in order to support PIM Bidir.

- For Cisco Nexus 9300 Series switches, make sure that the mask length for Bidir ranges is equal to or greater than 24 bits.

Guidelines and Limitations for PIM and PIM6

PIM and PIM6 have the following guidelines and limitations:

- Cisco NX-OS PIM and PIM6 are supported on Cisco Nexus 9300-EX, Cisco Nexus 9300-FX, Cisco Nexus 9300-FX2, and Cisco Nexus 9300-FX3S platform switches.
- Configuring a secondary IP address as an RP address is not supported.
- For most Cisco Nexus devices, RPF failure traffic is dropped and sent to the CPU at a very low rate to trigger PIM asserts. For the Cisco Nexus 9000 Series switches, RPF failure traffic is always copied to the CPU in order to learn multicast sources.
- For first-hop source detection in most Cisco Nexus devices, traffic coming from the first hop is detected based on the source subnet check, and multicast packets are copied to the CPU only if the source belongs to the local subnet. The Cisco Nexus 9000 Series switches cannot detect the local source, so multicast packets are sent to the supervisor to learn the local multicast source.
- Cisco NX-OS PIM and PIM6 do not interoperate with any version of PIM dense mode or PIM Sparse Mode version 1.
- PIM SSM and PIM ASM is supported on all Cisco Nexus 9000 Series switches.
- Cisco Nexus 9000 Series switches support PIM SSM on vPCs.
- It is recommended to configure a snooping querier on a L2 device with lower IP address to force the L2 device as the querier. This will be useful in handling the scenario where multi chassis EtherChannel trunk (MCT) is down.
- When the Rendezvous Point receives a PIM Data Register, it is expected for the register to be punted up to the CPU for processing. During this operation, the register will be decapsulated and the data portion of it will be software forwarded if there are any relevant OIFs for the group.
- (S,G) route is created on the control plane when data packet is punted regardless of spt-threshold infinity configuration. The route is created to protect the control plane and limit further punting of packets.
- If the NAT flows are established before the service interface is created as shown below, use the **clear ip mroute** *group source* command to manually clear the affected routes:

```
2024 Jan 30 15:26:17.127933 MFX2-4
%IPFIB-SLOT1-2-MFIB_EGR_NAT_INVALID_INTF: Service Intf Ethernet1/31.100
```

```
not available, Impacted translation flow:
(118.4.0.1,2.1.13.153)->(228.4.11.49,204.0.1.59)L4(0,0)2024 Jan 30
15:26:23.039119 MFX2-4 %ETHPORT-5-IF_UP: Interface Ethernet1/31.100
is up in Layer3
```

- Beginning with Cisco NX-OS Release 9.2(3):
  - PIM6 on TOR is supported in multicast heavy, ext-heavy, and default templates.
  - PIM6 on the Cisco Nexus 9500 boxes with EX/FX/GX line cards is only supported in multicast heavy, ext-heavy, dual-stack-multicast templates.
- Beginning with Cisco NX-OS Release 9.3(3), PIM6 support for SVI is introduced on TOR with or without vPC for switches ending with "EX", "FX", "FX2" and on EOR for switches ending with "EX", "FX".
- PIM6 support on SVI is possible only after the MLD snooping is enabled.
- Beginning with Cisco NX-OS Release 9.3(5), PIM6 support for SVI is introduced on Cisco Nexus 9300-GX platform switches and Cisco Nexus 9500 platform switches.
- Cisco Nexus 9000 Series switches support PIM ASM and SSM on vPCs.
- Cisco Nexus 9000 Series switches do not support PIM adjacency with a vPC leg or with a router behind a vPC.
- PIM Snooping is not supported on Cisco Nexus 9000 Series switches.
- Cisco Nexus 9000 Series switches support PIM6 ASM and SSM.



Note Only Cisco Nexus 9500 Series switches with N9K-X9400 or N9K-X9500 line cards and/or N9K-C9504-FM, N9K-C9508-FM, and N9K-C9516-FM fabric modules support PIM6 ASM and SSM. Cisco Nexus 9500 Series switches with other line cards or fabric modules do not support PIM6.

- PIM bidirectional multicast source VLAN bridging is not supported on FEX ports.
- PIM6 Bidirectional is supported.
- PIM6 is not supported on SVIs prior to Cisco NX-OS Release 9.3(3).
- PIM6 is not supported on any FEX ports (Layer 2 and Layer 3).
- PIM Bidirectional is supported for Cisco Nexus 9300-EX, Cisco Nexus 9300-FX/FX2/FX3, Cisco Nexus 9300-GX/GX2, Cisco Nexus 9300-H1/H2R platform switches.
- Cisco Nexus 9000 Series switches do not support PIM and PIM6 Bidir on vPCs or PIM6 ASM, SSM, and Bidirectional on vPCs.
- The PIM and PIM6 Bidir protocol has the following limitations:
  - By design there must be exactly one router acting as DF on every link.
  - If no routers are DF, the packets will drop.
  - If multiple routers are DF, the packets may be duplicated or looped.

  - When there is topology change, one router may stop being the DF, and a different router becomes the new DF.
  - During topology changes, although the PIM DF election is quick, many multicast routes may be affected. The time required to process all the affected routes and updating the forwarding plane, depends on the number of routes that are affected and may vary from a few milliseconds with a few routes, to more than a minute with thousands of routes.

- The following devices support PIM and PIM6 sparse mode on Layer 3 port-channel subinterfaces:
  - Cisco Nexus 9300 Series switches
  - Cisco Nexus 9300-EX Series switches and Cisco Nexus 3232C and 3264Q switches
  - Cisco Nexus 9500 Series switches with N9K-X9400 or N9K-X9500 line cards and/or N9K-C9504-FM, N9K-C9508-FM, and N9K-C9516-FM fabric modules.
- The multicast heavy template supports real-time packets and byte statistics but does not support VXLAN and tunnel egress or ingress statistics.
- Real-time/flex statistics is supported in:
  - Default template with configuration of **hardware profile multicast flex-stats-enable** command.
  - Heavy template without any configuration.

  Real-time statistics does not support ext-heavy template.
- GRE tunnels over IPv4 support multicast. GRE tunnels over IPv6 do not support multicast.
- Only Cisco Nexus 9300-EX and 9300-FX/FX2/FX3 platform switches support multicast on GRE tunnels.
- Beginning with Cisco NX-OS Release 10.2(1q)F, Multicast GRE is supported on Cisco Nexus N9KC9332D-GX2B platform switches.
- GRE tunnels does not support host connectivity.
- Because the IGMP functionality is not supported as part of the host connectivity, IGMP CLI is not available on GRE tunnels.
- You may not be able to add static tunnel OIFs to multicast routes, because IGMP CLI is not available on GRE tunnels, and it requires to statically bind a multicast group to the outgoing interface (OIF).
- Do not use SVI IP address as tunnel source or tunnel destination.
- Tunnel destination must be reachable via L3 physical interface or L3 subinterface.
- The L3 physical interface or subinterface via which the tunnel destination is reachable must be PIM enabled.
- Multiple GRE tunnels on the same device should not use the same source or the same destination.
- ECMP load sharing of GRE-encapsulated multicast traffic is not supported. If the tunnel destination is reachable across several links, the traffic is sent to only one of them.
- The multicast consistency checker is not supported on GRE tunnels.
- GRE tunnel can be a member of a VRF only if the source or destination interfaces are members of the same VRF.

- Multicast VRF-Lite Route Leaking is not supported for GRE.
- PIM Bidir is not supported with GRE.
- The Cisco Nexus 3232C and 3264Q switches do not support PIM6.
- When there is no PIM/PIM6 neighbor on an interface, the interface could be selected as an RPF interface based on the shortest/ECMP paths. Make sure to enable PIM/PIM6 on both the sides of the link when there are multiple ECMPs between the source and the receiver.
- Beginning with Cisco NX-OS Release 9.3(6), Multicast over GRE is supported on Cisco Nexus 9300-GX platform switches.
- Beginning with Cisco NX-OS Release 9.3(6), the following is supported:
  - Incoming RPF interface in Switch-1 is under default VRF and in Switch-2 on the other VRF.
  - Tunnel interface in Switch-1 is under default VRF and in Switch-2 on the other VRF.
  - Outgoing interface in Switch-1 is on the other VRF and in Switch-2 under default VRF.
- The presence of any GRE tunnel on the Cisco Nexus 9000 switches cannot co-exist with a sub-interface or with L3-routed multicast forwarded through an SVI to a trunk interface (multicast forwarding to a sub-interface or trunk port may be missing the dot1q tag). This impacts the receiving of multicast traffic connected via sub-interface and trunk-connected hosts. Traffic will be received at the parent interface and not at the sub-interface, or treated as native VLAN depending on the receiver configuration. This impact is only for regular/native multicast packets and not for Multicast GRE (encapsulation and decapsulation) packets. This limitation is applicable only to Cisco Nexus 9300-GX platform switches.
- The presence of any tunnel (feature tunnel or feature nv overlay) cannot co-exist with a sub-interface or with L3-routed multicast forwarded through an SVI to a trunk interface (multicast forwarding to a sub-interface or trunk port may be missing the dot1q tag) ; this will impact receiver on the other end. Traffic will be received at the parent interface and not at the sub-interface, or treated as native VLAN depending on the receiver configuration. This limitation is applicable only to Cisco Nexus 9300-GX platform switches.
- In case GRE tunnel's sources or destinations were misconfigured (such as having incompatible sources/destinations) they will be automatically shut down, and stay shut down even after the configuration has been recovered. The workaround is to manually shut/unshut such tunnels.
- In PIM-SM, some duplication or drops of packets are expected behavior when there are changes in the forwarding path. This behavior results in the following undesirable conditions:
  - When switching from receiving on the shared tree to shortest path tree (SPT), there is typically a small window when packets get dropped. The SPT feature may prevent this, but it may cause duplication sometimes.
  - The RP which initially forward packets that it may have received via PIM registers or MSDP will next join the SPT for native forwarding, and there is a small window where the RP may forward the same data packet twice, once as a native packet and once after PIM register or MSDP decap.

  To resolve these issues, ensure that the forwarding path does not change by configuring a long (S,G) expiration time or by using SSM/PIM Bidir.
- Beginning with Cisco NX-OS Release 10.3(1)F, PIM is supported on Cisco Nexus 9808 platform switches.

  - Beginning with Cisco NX-OS Release 10.4(1)F, PIM is supported on Cisco Nexus X98900CD-A and X9836DM-A line cards with Cisco Nexus 9808 switches.

- Beginning with Cisco NX-OS Release 10.4(1)F, PIM is supported on Cisco Nexus 9804 platform switches, and Cisco Nexus X98900CD-A and X9836DM-A line cards.
- PFM-SD has the following guidelines and limitations:
  - Policy based PFM-SD administrative boundary evaluation is not supported.
  - No multisite support
  - The PFM-SD mode can be enabled per VRF and for a set of group ranges. The PFM-SD mode is not enabled by default.
  - Do not configure RP for PFM-SD ranges.
  - With PMN multiple sources per group bandwidth management is not supported.
- PIM must be configured on all L3 interfaces between sources, receivers, and rendezvous points (RPs).
- If PIM is not enabled on the upstream router's interface, then traffic will be dropped.
- HSRP-aware PIM is not supported in Cisco NX-OS.
- When a Multicast enabled BL is being reloaded, it is necessary to ensure that the customer has a Fabric port tracking timer set to around 3 - 5 depending on route scale.

  The fabric port tracking ensures that L3out comes up late and hence would delay the unicast convergence wrt the routes through the L3out. This would provide sufficient time for PIM overload timer (3 min) to complete and be ready to handle multicast states and data streams and Stripe winner related duties.

  Note that increasing port tracking would not affect any data streams currently running, since the expectation is that while the reloaded BL is still coming up, an alternate or backup BL is handling the data streams and performing Stripe winner related duties.
- Beginning with Cisco NX-OS Release 10.6(1)F, the ip pim spt-switch-graceful command is enabled by default. To disable the command, use no ip pim spt-switch-graceful command. This feature minimizes packet loss by allowing a graceful switchover from the shared tree to the shortest path tree (SPT) where the shared tree is used until the shortest path tree (SPT) is fully established and verified by receiving the first data packet.
  - In the earlier releases, this command is not enabled by default.
  - This feature is not supported for TRM VRF.
  - This feature is not supported for SVI as RPF.
  - This feature is not supported on VPC.
- During high-rate multicast forwarding, the number of packets reported as software-switched (`show ip mroute summary software-forwarded vrf all`) may be lower than the number of packets reported as transmitted in COPP statistics. Some initial packets may not be accounted for in either hardware or software-switched counters, and a small amount of packet loss is expected for a short time until the multicast route (mroute) is programmed in hardware. This is normal behavior and should be considered when interpreting multicast forwarding statistics.

- Beginning with Cisco NX-OS Release 10.6(3)F, support is added for PIM6 Bidir on Cisco Nexus 9300-FX/FX2/FX3/GX/GX2/HX switches and Cisco Nexus 9700-EX/FX/GX/FX3 line cards.

Guidelines and Limitations on N9300-Series Smart Switches

Beginning with Cisco NX-OS Release 10.6(2)F, Layer 2 and Layer 3 IPv4 multicast PIM (ASM, SSM) are supported on the Cisco Nexus N9324C-SE1U and N9348Y2C6D-SE1U switches.

Guidelines and Limitations for Hello Messages

The following guidelines and limitations apply to Hello Messages:

- Default values for the PIM hello interval are recommended and should not be modified.

Guidelines and Limitations for Rendezvous Points

The following guidelines and limitations apply to Rendezvous Points (RP):

- Configure candidate RP intervals to a minimum of 15 seconds.
- Do not configure both Auto-RP and BSR protocols in the same network.
- PIM6 does not support BSRs and Auto-RP.
- You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM and PIM6 Bidir RP.
- For all Cisco NX-OS 7.x and later releases, the loopback interface that is used to configure RP in multicast must have the **ip**[**v6**] **pimsparse-mode** configuration.
- The interface that is used to configure a PIM RP (whether static, BSR or Auto-RP) must have **ip** [**v6**] **pim sparse-mode**.
- To avoid excessive punts of the RPF failed packets, the Cisco Nexus 9000 Series switches may create S, G entries for active sources in ASM, although there is no rendezvous point (RP) for such group, or in situation when a reverse path forwarding (RPF) fails for the source.

  This behavior does not apply to Nexus 9200, 9300-EX platform switches, and N9K-X9700-EX LC platforms.
- 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.
- If the source VRF forwards multicast traffic across to a non-forwarder vPC peer which happens to be RP, then the S,G entries are not created on the forwarder vPC peer. This can lead to a drop in the multicast traffic for these sources. In order to avoid this, you must configure a anycast RP in the topology wherever the vPC peer is also a RP.

Guidelines and Limitations for Multicast VRF-lite Route Leaking

The following guidelines and limitations apply to multicast VRF-lite route leaking:

- Cisco Nexus 9000 Series switches support multicast VRF-lite route leaking.
- Multicast VRF-lite route leaking is not supported on Cisco Nexus 9500 platform switches with -R or -RX line cards.
- PIM Sparse Mode and PIM SSM are supported with multicast VRF-lite route leaking. However, PIM SSM with vPC is not supported with multicast VRF-lite route leaking.
- Only static rendezvous points (RPs) are supported with multicast VRF-lite route leaking.
- The source and rendezvous point (RP) should be in the same VRF.

Default Settings

This table lists the default settings for PIM and PIM6 parameters.

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

Parameters	Default
SSM multicast group range or policy	**IPv4** • 232.0.0.0/8 **IPv6** • ff32::/32 • ff33::/32 • ff34::/32 • ff35::/32 • ff36::/32 • ff37::/32 • ff38::/32 • ff39::/32 • ff3a::/32 • ff3b::/32 • ff3c::/32 • ff3d::/32 • ff3e::/32
PIM sparse mode	Disabled
Designated router priority	1
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
BFD	Disabled

Configuring PIM and PIM6

You can configure PIM for each interface.

You can configure both PIM and PIM6 on the same router. You can 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	Source-Specific Multicast
RPF routes for multicast	No	RPF routes for multicast

PIM and PIM6 Configuration Tasks

The following steps configure PIM and PIM6.

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

Note The CLI commands used to configure PIM are as follows:

- Configuration commands begin with **ip pim** for PIM and with **ipv6 pim** for PIM6.
- Show commands begin with **show ip pim** for PIM and with **show ipv6 pim** for PIM6.

Enabling the PIM and PIM6 Feature

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



Note Beginning with Cisco NX-OS Release 7.0(3)I5(1), you no longer need to enable at least one interface with IP PIM sparse mode in order to enable PIM or PIM6.

Before you begin

Ensure that you have installed the Enterprise Services license.

SUMMARY STEPS

1. **configure terminal**
2. **feature pim**
3. **feature pim6**
4. (Optional) **show running-configuration pim**
5. (Optional) **show running-configuration pim6**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`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	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Shows the running-configuration information for PIM.
Step 5	(Optional) **show running-configuration pim6** **Example:**	Shows the running-configuration information for PIM6.

	Command or Action	Purpose
	`switch(config)# show running-configuration pim6`	
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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 for and forwarding of Auto-RP messages. The default is disabled, which means that the router does not listen for 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 for and forwarding of BSR messages. The default is disabled, which means that the router does not listen for or forward BSR messages unless it is configured as a candidate RP or BSR candidate. **Note** PIM6 does not support BSR.
Bidir RP limit	Configures the number of Bidir RPs that you can configure for IPv4. The maximum number of Bidir RPs supported per VRF for PIM cannot exceed 8. Values range from 0 to 8. The default is 6. **Note** Only applicable to PIM.
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 multi-access 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.
Designated router delay	Delays participation in the designated router (DR) election by setting the DR priority that is advertised in PIM hello messages to 0 for a specified period. During this delay, no DR changes occur, and the current switch is given time to learn all of the multicast states on that interface. After the delay period expires, the correct DR priority is sent in the hello packets, which retriggers the DR election. Values range from 3 to 0xffff seconds.
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 MD5 authentication.
Hello authentication keychain	Enables the keychain authentication on a PIM interface. Where <keychain> is the name of a keychain. **Note** PIM6 does not support keychain 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 9000 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 prefix-list policy.[1] If the policy name does not exist or no prefix lists 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. **Note** The PIM neighbor policy supports only prefix lists. It does not support ACLs used inside a route map.

[1] To configure prefix-list policies, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Configuring PIM Sparse Mode Parameters

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]}
3. (Optional) **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]}
4. (Optional) **ip pim bidir-rp-limit** *limit*
5. (Optional) **ip pim register-rate-limit** *rate*
6. (Optional) **ip pim spt-threshold infinity group-list** *route-map-name*
7. (Optional) [**ip** | **ipv4**] **routing multicast holddown** *holddown-period*
8. (Optional) **show running-configuration pim**
9. **interface** *interface*
10. **ip pim sparse-mode**
11. (Optional) **ip pim dr-priority** *priority*
12. (Optional) **ip pim dr-delay** *delay*
13. (Optional) **ip pim hello-authentication ah-md5** *auth-key*
14. (Optional) **ip pim hello-authentication keychain** *name*
15. (Optional) **ip pim hello-interval** *interval*
16. (Optional) **ip pim border**
17. (Optional) **ip pim neighbor-policy prefix-list** *prefix-list*
18. (Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]
19. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	(Optional) **ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]} **Example:** `switch(config)# ip pim auto-rp listen`	Enables listening for or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen for or forward Auto-RP messages.
Step 3	(Optional) **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} **Example:** `switch(config)# ip pim bsr forward`	Enables listening for or forwarding of BSR messages. The default is disabled, which means that the software does not listen for or forward BSR messages.
Step 4	(Optional) **ip pim bidir-rp-limit** *limit* **Example:** `switch(config)# ip pim bidir-rp-limit 4`	Specifies the number of Bidir RPs that you can configure for IPv4. The maximum number of Bidir RPs supported per VRF for PIM cannot exceed 8. Values range from 0 to 8. The default value is 6.
Step 5	(Optional) **ip pim register-rate-limit** *rate* **Example:** `switch(config)# ip pim register-rate-limit 1000`	Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 6	(Optional) **ip pim spt-threshold infinity group-list** *route-map-name* **Example:** `switch(config)# ip pim spt-threshold infinity group-list my_route-map-name`	Creates the IPv4 PIM (*, G) state only, for the group prefixes defined in the specified route map. Cisco NX-OS Release 3.1 supports up to 1000 route-map entries, and Cisco NX-OS releases prior to 3.1 support up to 500 route-map entries. **Note** The **ip pim use-shared-tree-only group-list** command performs the same function as the **ip pim spt-threshold infinity group-list** command. You can choose to use either command to implement this step. Both the commands (**ip pim spt-threshold infinity group-list** and **ip pim use-shared-tree-only group-list** has the following limitations: • It is only supported for virtual port channels (vPC) on the Cisco Nexus 9000 Cloud Scale Switches. • It is supported in NX-OS (non-vPC) Last Hop Router (LHR) configurations.

	Command or Action	Purpose
Step 7	(Optional) [**ip** | **ipv4**] **routing multicast holddown** *holddown-period* **Example:** `switch(config)# ip routing multicast holddown 100`	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	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	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 configuration mode.

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	(Optional) **ip pim dr-priority** *priority* **Example:** `switch(config-if)# ip pim dr-priority 192`	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	(Optional) **ip pim dr-delay** *delay* **Example:** `switch(config-if)# ip pim dr-delay 3`	Delays participation in the designated router (DR) election by setting the DR priority that is advertised in PIM hello messages to 0 for a specified period. During this delay, no DR changes occur, and the current switch is given time to learn all of the multicast states on that interface. After the delay period expires, the correct DR priority is sent in the hello packets, which retriggers the DR election. Values range from 3 to 0xffff seconds. **Note** This command delays participation in the DR election only upon bootup or following an IP address or interface state change. It is intended for use with multicast-access non-vPC Layer 3 interfaces only.
Step 13	(Optional) **ip pim hello-authentication ah-md5** *auth-key* **Example:** `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	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.

	Command or Action	Purpose
Step 14	(Optional) **ip pim hello-authentication keychain** *name* **Example:** `switch(config-if)# ip pim hello-authentication keychain mykeychain`	Enables the keychain authentication on a PIM interface. Where <keychain> is the name of a keychain. **Note** • Authentication can be configured with specific keychain name before the keychain is configured, but authentication will pass only if the keychain is present with a valid key. • If keychain authentication is configured, the old password based authentication will be ignored if present.
Step 15	(Optional) **ip pim hello-interval** *interval* **Example:** `switch(config-if)# ip pim hello-interval 25000`	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000. **Note** The minimum value is 1 millisecond.
Step 16	(Optional) **ip pim border** **Example:** `switch(config-if)# ip pim 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.
Step 17	(Optional) **ip pim neighbor-policy prefix-list** *prefix-list* **Example:** `switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix`	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. Also configures which PIM neighbors to become adjacent to based on a prefix-list policy with the **ip prefix-list** *prefix-list* command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 18	(Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	Displays PIM interface information.
Step 19	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring PIM6 Sparse Mode Parameters

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **ipv6 pim register-rate-limit** *rate*
3. (Optional) **ipv6 routing multicast holddown** *holddown-period*
4. (Optional) **show running-configuration pim6**
5. **interface** *interface*
6. **ipv6 pim sparse-mode**
7. (Optional) **ipv6 pim dr-priority** *priority*
8. (Optional) **ipv6 pim hello-interval** *interval*
9. (Optional) **ipv6 pim border**
10. (Optional) **ipv6 pim neighbor-policy prefix-list** *prefix-list*
11. **show ipv6 pim interface** [*interface* | brief] [vrf *vrf-name* | all]
12. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	(Optional) **ipv6 pim register-rate-limit** *rate* **Example:** `switch(config)# ipv6 pim register-rate-limit 1000`	Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 3	(Optional) **ipv6 routing multicast holddown** *holddown-period* **Example:** `switch(config)# ipv6 routing multicast holddown 100`	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 4	(Optional) **show running-configuration pim6** **Example:** `switch(config)# show running-configuration pim6`	Displays PIM6 running-configuration information, including the register rate limit.

Step 5	**interface** *interface*
	Example:
	`switch(config)# interface vlan 10`
	`switch(config-if)#`
		Enters interface configuration mode on the specified interface.

	Command or Action	Purpose
Step 6	**ipv6 pim sparse-mode** **Example:** `switch(config-if)# ipv6 pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled. Beginning with Cisco NX-OS Release 9.3(5) you can configure this command on a SVI interface in Broadcom-based switches.
Step 7	(Optional) **ipv6 pim dr-priority** *priority* **Example:** `switch(config-if)# ipv6 pim dr-priority 192`	Sets the designated router (DR) priority that is advertised in PIM6 hello messages. Values range from 1 to 4294967295. The default is 1.
Step 8	(Optional) **ipv6 pim hello-interval** *interval* **Example:** `switch(config-if)# ipv6 pim hello-interval 25000`	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000.
Step 9	(Optional) **ipv6 pim border** **Example:** `switch(config-if)# ipv6 pim border`	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.
Step 10	(Optional) **ipv6 pim neighbor-policy prefix-list** *prefix-list* **Example:** `switch(config-if)# ipv6 pim neighbor-policy prefix-list AllowPrefix`	Configures which PIM6 neighbors to become adjacent to based on a prefix-list policy with the **ipv6 prefix-list** *prefix-list* command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM6 neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 11	**show ipv6 pim interface** [*interface* | brief] [vrf *vrf-name* | all] **Example:** `switch(config-if)# show ipv6 pim interface`	Displays PIM6 interface information.
Step 12	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring PIM Flooding Mechanism with Source Discovery

Follow this procedure to configure PFM-SD:

SUMMARY STEPS

1. **configure terminal**
2. **[no] ip pim pfm-sd range** {*prefix* | { **route-map** *route-map-name* } | { **prefix-list** *prefix-list-name* }}

3. **[no] ip pim pfm-sd originator-id** {*interface*}
4. **[no] ip pim pfm-sd announcement interval** { *interval* }
5. **[no] ip pim pfm-sd announcement gap** { *interval* }
6. **[no] ip pim pfm-sd announcement rate** { *rate* }
7. [no] ip pim pfm-sd gsh holdtime { holdtime }
8. **interface** {*interface port*}
9. **[no] ip pim pfm-sd** {**boundary** [*direction*]}
10. **end**
11. (Optional) **show ip pim pfm-sd** { **cache** [*local*] | [*remote-discovery*]]}
12. (Optional) **show ip pim interface** {*interface port*}
13. (Optional) **show ip pim vrf internal**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**[no] ip pim pfm-sd range** {*prefix* | { **route-map** *route-map-name* } | { **prefix-list** *prefix-list-name* }} **Example:** `switch(config)# ip pim pfm-sd range route-map r1`	Enables PFM-SD for a given multicast group range. Up to 10 ranges are supported in a route map/prefix list.
Step 3	**[no] ip pim pfm-sd originator-id** {*interface*} **Example:** `switch(config)# ip pim pfm-sd originator-id lo5`	Configures originator for PFM-SD announcements.
Step 4	**[no] ip pim pfm-sd announcement interval** { *interval* } **Example:** `switch(config)# ip pim pfm-sd announcement interval 170`	Configure periodicity of announcements. The default interval value is 60 seconds.
Step 5	**[no] ip pim pfm-sd announcement gap** { *interval* } **Example:** `switch(config)# ip pim pfm-sd announcement gap 1600`	Configures a gap between the PFM-SD messages that are sent. The default interval value is 1000 milliseconds.
Step 6	**[no] ip pim pfm-sd announcement rate** { *rate* } **Example:** `switch(config)# ip pim pfm-sd announcement rate 10`	Configures the PFM-SD message rate per interface. The default rate is 6.

	Command or Action	Purpose
Step 7	[no] ip pim pfm-sd gsh holdtime { holdtime } **Example:** `switch(config)# ip pim pfm-sd gsh holdtime 250`	Configures the PFM-SD source holdtime. The default holdtime is 210 seconds.

Step 8	**interface** {*interface port*}
	Example:
	`switch(config)# interface eth1/1`
	`switch(config-if)#`
		Configures an interface and enters interface configuration mode.

Step 9	**[no] ip pim pfm-sd** {**boundary** [*direction*]} **Example:** `switch(config-if)# ip pim pfm-sd boundary in`	Configures the PFM-SD boundary. Both **in**, **out**, and **both** options are available for direction.

Step 10	**end**
	Example:
	`switch(config-if)# end`
	`switch#`
		Exits interface configuration mode and enters the privileged EXEC mode.

Step 11	(Optional) **show ip pim pfm-sd** { **cache** [*local*] | [*remote-discovery*]]} **Example:** `switch# show ip pim pfm-sd cache local`	Displays PIM PFM-SD local or Remote Discovery cache information.
Step 12	(Optional) **show ip pim interface** {*interface port*} **Example:** `switch# show ip pim interface ethernet 1/17`	Displays the PIM interface status for the VRF.
Step 13	(Optional) **show ip pim vrf internal** **Example:** `switch# show ip pim vrf internal`	Displays the PIM enabled VRFs.

Configuring ASM and Bidir

Any Source Multicast (ASM) is a multicast distribution mode that requires the use of RPs to act as a shared root between sources and receivers of multicast data.

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.

Configuring Static RPs

You can configure an RP statically by configuring the RP address on every router that will participate 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 or specify a prefix-list method of configuration.

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
```

Configuring Static RPs (PIM)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **prefix-list** *name* |**override** |**route-map** *policy-name*] [**bidir**]
3. (Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix*	**prefix-list** *name* |**override** |**route-map** *policy-name*] [**bidir**] **Example:**	Configures a PIM static RP address for a multicast group range.

	Command or Action	Purpose
	`switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9` `ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/96`	You can specify a prefix-list policy name for the static RP address or 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 **override** option causes the RP address to override the dynamically learned RP addresses for specified groups in route-map. The example configures PIM ASM mode for the specified group range.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM RP information, including BSR listen and forward states.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Static RPs (PIM6)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* | **route-map** *policy-nsmr*]
3. (Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* | **route-map** *policy-nsmr*] **Example:**	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 or Action	Purpose
	`switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/24`	command. The mode is ASM. The default group range is ff00::0/8. The example configures PIM6 ASM mode for the specified group range.
Step 3	(Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ipv6 pim group-range`	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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 in the table below.

Note PIM6 does not support BSRs.

Table 3: Candidate BSR Arguments

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

Configuring BSRs Candidate RP Arguments and Keywords

You can configure a candidate RP with the arguments and keywords described in 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 boots 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 f 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 1 seconds.
priority	Priority assigned to this RP. The software elects the RP with the highest priority 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 prio to 255 and has a default of 192. **Note** This priority differs from the BSR BSR-candidate priority, which prefers the high value between 0 and 255.
bidir	Unless you specify bidir, this RP will be in ASM mode. If you specify bidir, the will be in Bidir mode.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is app

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 for and forward BSR messages. A router configured as either a candidate RP or a candidate BSR will automatically listen for and forward all bootstrap router protocol messages, unless an interface is configured with the domain border feature.
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.

Configuring BSRs (PIM)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ip pim bsr** {**forward** [**listen**] | **listen** [**forward**]}
3. **ip pim bsr bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*]
4. **ip pim sparse-mode**
5. (Optional) **ip pim bsr rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* [**bidir**]
6. (Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim bsr** {**forward** [**listen**]	**listen** [**forward**]} **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*] [**priority** *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-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 5	(Optional) **ip pim bsr rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* [**bidir**] **Example:** `switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	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. Use the **bidir** option to create a Bidir candidate RP. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.

	Command or Action	Purpose
Step 6	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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 in 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.

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 in 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.

Argument or Keyword	Description
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.
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 for and forward Auto-RP messages. A router configured as either a candidate RP or an Auto-RP mapping agent will automatically listen for and forward all Auto-RP protocol messages, unless an interface is configured with the domain border feature.
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.

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

Configuring Auto RP (PIM)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ip pim** {**send-rp-discovery** | **auto-rp mapping-agent**} *interface* [**scope** *ttl*]
3. **ip pim** {**send-rp-announce** | **auto-rp rp-candidate**} *interface* {**group-list** *ip-prefix* | **prefix-list** *name* | **route-map** *policy-name*} [**scope** *ttl*] **interval** *interval*] [**bidir**]
4. **ip pim sparse-mode**
5. (Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]

6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim** {**send-rp-discovery** | **auto-rp mapping-agent**} *interface* [**scope** *ttl*] **Example:** `switch(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**} *interface* {**group-list** *ip-prefix* | **prefix-list** *name* | **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`	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. Use the **bidir** option to create a Bidir candidate RP. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 4	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 5	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *number*
3. **ip address** *ip-prefix*
4. **ip pim sparse-mode**
5. **ip router** *routing-protocol-configuration*
6. **exit**
7. **interface loopback** *number*
8. **ip address** *ip-prefix*
9. **ip pim sparse-mode**
10. **ip router** *routing-protocol-configuration*
11. **exit**
12. **ip pim rp-address** *anycast-rp-address* [**group-list** *ip-address*]
13. **ip pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address*
14. Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).
15. (Optional) **show ip pim rp**
16. (Optional) **show ip mroute** *ip-address*
17. (Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
18. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		Configures an interface loopback.
		This example configures interface loopback 0.

	Command or Action	Purpose
Step 3	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 192.168.1.1/32`	Configures an IP address for this interface. It should be a unique IP address that helps to identify this router.
Step 4	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode.
Step 5	**ip router** *routing-protocol-configuration* **Example:** `switch(config-if)# ip router ospf 1 area 0.0.0.0`	Enables the interface to be reachable by other routers in the Anycast RP set.

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 7	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 1`
	`switch(config-if)#`
		Configures an interface loopback.
		This example configures interface loopback 1.

Step 8	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 10.1.1.1/32`	Configures an IP address for this interface. It should be a common IP address that acts as the Anycast RP address.
Step 9	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 10	**ip router** *routing-protocol-configuration* **Example:** `switch(config-if)# ip router ospf 1 area 0.0.0.0`	Enables the interface to be reachable by other routers in the Anycast RP set.

Step 11	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 12	**ip pim rp-address** *anycast-rp-address* [**group-list** *ip-address*] **Example:** `switch(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4`	Configures the PIM Anycast RP address.

	Command or Action	Purpose
Step 13	**ip pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address* **Example:** `switch(config)# ip pim anycast-rp 10.1.1.1 192.168.1.1`	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 14	Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).	—
Step 15	(Optional) **show ip pim rp** **Example:** `switch(config)# show ip pim rp`	Displays the PIM RP mapping.
Step 16	(Optional) **show ip mroute** *ip-address* **Example:** `switch(config)# show ip mroute 239.1.1.1`	Displays the mroute entries.
Step 17	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 18	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a PIM Anycast RP Set (PIM6)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *number*
3. **ipv6 address** *ipv6-prefix*
4. **ipv6 pim sparse-mode**
5. **ipv6 router** *routing-protocol-configuration*
6. **exit**
7. **interface loopback** *number*
8. **ipv6 address** *ipv6-prefix*
9. **ipv6 router** *routing-protocol-configuration*
10. **exit**
11. **ipv6 pim rp-address** *anycast-rp-address* [**group-list** *ip-address*]
12. **ipv6 pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address*

13. Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).
14. (Optional) **show ipv6 pim rp**
15. (Optional) **show ipv6 mroute** *ipv6-address*
16. (Optional) **show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**]
17. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		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::5/32`	Configures an IP address for this interface. It should be a unique IP address that helps to identify this router.
Step 4	**ipv6 pim sparse-mode** **Example:** `switch(config-if)# ipv6 pim sparse-mode`	Enable PIM6 sparse mode.
Step 5	**ipv6 router** *routing-protocol-configuration* **Example:** `switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0`	Enables the interface to be reachable by other routers in the Anycast RP set.

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 7	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 1`
	`switch(config-if)#`
		Configures an interface loopback.
		This example configures interface loopback 1.

	Command or Action	Purpose
Step 8	**ipv6 address** *ipv6-prefix* **Example:** `switch(config-if)# ipv6 address 2001:0db8:0:abcd::1111/32`	Configures an IP address for this interface. It should be a common IP address that acts as the Anycast RP address.
Step 9	**ipv6 router** *routing-protocol-configuration* **Example:** `switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0`	Enables the interface to be reachable by other routers in the Anycast RP set.

Step 10	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 11	**ipv6 pim rp-address** *anycast-rp-address* [**group-list** *ip-address*] **Example:** `switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1111 group-list ff1e:abcd:def1::0/24`	Configures the PIM6 Anycast RP address.
Step 12	**ipv6 pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address* **Example:** `switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111`	Configures a PIM6 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 13	Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).	—
Step 14	(Optional) **show ipv6 pim rp** **Example:** `switch(config)# show ipv6 pim rp`	Displays the PIM RP mapping.
Step 15	(Optional) **show ipv6 mroute** *ipv6-address* **Example:** `switch(config)# show ipv6 mroute ff1e:2222::1:1:1:1`	Displays the mroute entries.
Step 16	(Optional) **show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ipv6 pim group-range`	Displays PIM6 modes and group ranges.
Step 17	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

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

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 9000 Series NX-OS Interfaces Configuration Guide*.

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.

SUMMARY STEPS

1. **configure terminal**
2. **ip pim use-shared-tree-only group-list** *policy-name*
3. (Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim use-shared-tree-only group-list** *policy-name* **Example:**	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

	Command or Action	Purpose
	`switch(config)# ip pim use-shared-tree-only group-list my_group_policy`	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. This command has the following limitations: • It is only supported for virtual port channels (vPC) on the Cisco Nexus 9000 Cloud Scale Switches. • It is supported in NX-OS (non-vPC) Last Hop Router (LHR) configurations.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Shared Trees Only for ASM (PIM6)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ipv6 pim use-shared-tree-only group-list** *policy-name*
3. (Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

Configuring SSM (PIM)

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 group-to-source mapping using SSM translation.

You can only configure the IPv4 group range that is used by SSM.



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

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | none} | route-map *policy-name*}
3. (Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	[**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | none} | route-map *policy-name*}
	Example:
	`switch(config)# ip pim ssm range 239.128.1.0/24`
	Example:
	`switch(config)# no ip pim ssm range none`
		The following options are available:
		• **prefix-list**—Specifies a prefix-list policy name for the SSM range.
		• **range**—Configures a group range for SSM. The default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed.
		• **route-map**—Specifies a route-map policy name that lists the group prefixes to use with the **match ip multicast** command.
		The **no** option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the keyword **none** is specified, the **no** command resets the SSM range to the default value of 232.0.0.0/8.
		Note
		You can configure a maximum of four ranges for SSM multicast, using the **prefix-list**, **range**, or **route-map** commands.

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

Configuring PIM SSM Over a vPC

Configuring PIM SSM over a vPC enables support for IGMPv3 joins and PIM S,G joins over vPC peers in the SSM range. This configuration is supported for orphan sources or receivers in the Layer 2 or Layer 3 domain. When you configure PIM SSM over a vPC, no rendezvous point (RP) configuration is required.

(S,G) entries will have the RPF as the interface toward the source, and no *,G states will be maintained in the MRIB.

Before you begin

Ensure that you have the PIM and vPC features enabled.

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

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *name*
3. (Optional) [**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | **none**} | **route-map** *policy-name*}
4. (Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**vrf context** *name*
	Example:
	`switch(config)# vrf context Enterprise`
	`switch(config-vrf)#`
		Creates a new VRF and enters VRF configuration mode. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.

Step 3	(Optional) [**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | **none**} | **route-map** *policy-name*} **Example:** `switch(config-vrf)# ip pim ssm range 234.0.0.0/24`	The following options are available: • **prefix-list**—Specifies a prefix-list policy name for the SSM range. • **range**—Configures a group range for SSM. The default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed. • **route-map**—Specifies a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. By default, the SSM range is 232.0.0.0/8. PIM SSM over vPC works as long as S,G joins are received in this range. If you want to override the default with some other range, you must specify that range using this command. The command in the example overrides the default range to 234.0.0.0/24. The **no** option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the

	Command or Action	Purpose
		keyword **none** is specified, the **no** command resets the SSM range to the default value of 232.0.0.0/8.
Step 4	(Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-vrf)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-vrf)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring RPF Routes for Multicast

You can define reverse path forwarding (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 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.

Note If the **ip multicast multipath s-g-hash** CLI is not configured, the multicast traffic may fail the RFP check.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* | *interface*} [*route-preference*] [**vrf** *vrf-name*]
3. (Optional) **show ip static-route** [**multicast**] [**vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`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 192.0.2.33/1 224.0.0.0/32`	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	(Optional) **show ip static-route** [**multicast**] [**vrf** *vrf-name*] **Example:** `switch(config)# show ip static-route multicast`	Displays configured static routes.
Step 4	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring Multicast Multipath

By default, the RPF interface for multicast is chosen automatically when multiple ECMP paths are available.

SUMMARY STEPS

1. **configure terminal**
2. **ip multicast multipath** {**none** | **resilient** | **s-g-hash**}
3. **clear ip mroute** *

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip multicast multipath** {**none** | **resilient** | **s-g-hash**} **Example:** `switch(config)# ip multicast multipath none`	Configure multicast multipath using the following options: • **none**—Disables multicast multipath by suppressing hashing across multiple ECMPs in the URIB RPF lookup. With this option, the highest RPF neighbor (next-hop) address is used for the RPF interface.

	Command or Action	Purpose
		Note Use the **ip multicast multipath none** command to completely disable hashing. • **s-g-hash**—Initiates S, G, nexthop hashing (rather than the default of S/RP, G-based hashing) to select the RPF interface. This option configures the hash based on source and group address. This is the default setting. • **resilient**—If the ECMP path list changes and the old RPF information is still part of the ECMP, this option uses the old RPF information instead of performing a rehash and potentially changing the RPF information. The **ip multicast multipath resilient** command is for maintaining resiliency (Stickiness) to the current RPF if there is a path in the route reachability notification from URIB. **Note** The **no ip multicast multipath resilient** command disables the stickiness algorithm. This command is independent of the hashing algorithm. **Note** For Cisco Nexus 9508 switches with the X9636C-R or X9636Q-R line card or the C9508-FM-R fabric module, if you want to change from the **resilient** option to the **none** option, first enter the **no ip multicast multipath resilient** command and then enter the **ip multicast multipath none** command.
Step 3	**clear ip mroute** * **Example:** `switch(config)# clear ip mroute *`	Clears multipath routes and activates multicast multipath suppression.

Configuring Multicast VRF-Lite Route Leaking

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure multicast VRF-lite route leaking, which allows IPv4 multicast traffic across VRFs.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-list*

3. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-list* **Example:** `switch(config)# ip multicast rpf select vrf blue group-list 236.1.0.0/16`	Specifies which VRF to use for RPF lookup for a particular multicast group. *src-vrf-name* is the name of the source VRF. It can be a maximum of 32 alphanumeric characters and is case sensitive. *group-list* is the group range for the RPF. The format is A.B.C.D/LEN with a maximum length of 32.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Route Maps to Control RP Information Distribution

You can configure route maps to help protect against some RP configuration errors and malicious attacks.

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.



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)

SUMMARY STEPS

1. **configure terminal**
2. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
3. **match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ip-prefix*} {**source** *source-ip-address*}
4. (Optional) **show route-map**

5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`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.

Step 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**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 Bidir`
		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 example.
		Note
		In the **match ip multicast group-range** <> CLI, the **group-range** command under **route-map** is not supported.

Step 4	(Optional) **show route-map** **Example:** `switch(config-route-map)# show route-map`	Displays configured route maps.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-route-map)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Route Maps to Control RP Information Distribution (PIM6)

SUMMARY STEPS

1. **configure terminal**
2. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
3. **match ipv6 multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ipv6-prefix*} {**source** *source-ip-address*}
4. (Optional) **show route-map**

5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`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)#`
		Enters route-map configuration mode.

Step 3	**match ipv6 multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ipv6-prefix*} {**source** *source-ip-address*} **Example:** `switch(config-route-map)# match ipv6 multicast group ff1e:abcd:def1::0/24 rp 2001:0db8:0:abcd::1 rp-type ASM`	Matches the group, RP, and RP type specified. You can specify the RP type (ASM). This configuration method requires the group and RP specified as shown in the example.
Step 4	(Optional) **show route-map** **Example:** `switch(config-route-map)# show route-map`	Displays configured route maps.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-route-map)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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	

Message Type	Description
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 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. **Note** PIM6 does not support BSRs.
BSR policy	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. **Note** PIM6 does not support BSRs.
Auto-RP candidate RP policy	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. **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 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. **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 policy 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 9000 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:

- The **jp-policy** command can use (S,G), (*,G), or (RP,G).
- The **register-policy** command can use (S,G) or (*,G).
- The **igmp report-policy** command can use (*,G) or (S,G).
- The **state-limit reserver-policy** command can use (*,G) or (S,G).
- The **auto-rp rp-candidate-policy** command can use (RP,G).
- The **bsr rp-candidate-policy** command can use (RP,G).
- The **autorp mapping-agent policy** command can use (S).
- The **bsr bsr-policy** command can use (S).

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

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

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **ip pim log-neighbor-changes**
3. (Optional) **ip pim register-policy** *policy-name*
4. (Optional) **ip pim bsr rp-candidate-policy** *policy-name*
5. (Optional) **ip pim bsr bsr-policy** *policy-name*
6. (Optional) **ip pim auto-rp rp-candidate-policy** *policy-name*
7. (Optional) **ip pim auto-rp mapping-agent-policy** *policy-name*
8. **interface** *interface*
9. (Optional) **ip pim jp-policy** *policy-name* [**in** | **out**]
10. (Optional) **show run pim**
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	(Optional) **ip pim log-neighbor-changes** **Example:** `switch(config)# ip pim log-neighbor-changes`	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	(Optional) **ip pim register-policy** *policy-name* **Example:** `switch(config)# ip pim register-policy my_register_policy`	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	(Optional) **ip pim bsr rp-candidate-policy** *policy-name* **Example:** `switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy`	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 ASM or Bidir 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	(Optional) **ip pim bsr bsr-policy** *policy-name* **Example:** `switch(config)# ip pim bsr bsr-policy my_bsr_policy`	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.
Step 6	(Optional) **ip pim auto-rp rp-candidate-policy** *policy-name* **Example:** `switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy`	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 ASM or Bidir 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	(Optional) **ip pim auto-rp mapping-agent-policy** *policy-name* **Example:** `switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy`	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:**	Enters interface mode on the specified interface.

	Command or Action	Purpose
	`switch(config)# interface ethernet 2/1` `switch(config-if)#`	
Step 9	(Optional) **ip pim jp-policy** *policy-name* [**in** | **out**] **Example:** `switch(config-if)# ip pim jp-policy my_jp_policy`	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.
Step 10	(Optional) **show run pim** **Example:** `switch(config-if)# show run pim`	Displays PIM configuration commands.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Message Filtering (PIM6)

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **ipv6 pim log-neighbor-changes**
3. (Optional) **ipv6 pim register-policy** *policy-name*
4. (Optional) **ipv6 pim jp-policy** *policy-name* [**in** | **out**]
5. (Optional) **show run pim6**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

	Command or Action	Purpose
Step 3	(Optional) **ipv6 pim register-policy** *policy-name* **Example:** `switch(config)# ipv6 pim register-policy my_register_policyinterface interfaceEnters interface mode on the specified interface. switch(config)# interface ethernet 2/1 switch(config-if)#`	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	(Optional) **ipv6 pim jp-policy** *policy-name* [**in** | **out**] **Example:** `switch(config-if)# ipv6 pim jp-policy my_jp_policy`	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. This command filters messages in both incoming and outgoing directions.
Step 5	(Optional) **show run pim6** **Example:** `switch(config-if)# show run pim6`	Displays PIM6 configuration commands.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Restarting the PIM and PIM6 Processes

When static RP is configured, you can restart the PIM processes and optionally flush all routes. By default, routes are not flushed.

Note When Auto-RP or BSR is configured, multicast traffic is dropped (for up to 60 seconds).

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

Before you begin

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

SUMMARY STEPS

1. **restart pim**
2. **configure terminal**
3. **ip pim flush-routes**
4. (Optional) **show running-configuration pim**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**restart pim** **Example:** `switch# restart pim`	Restarts the PIM process. **Note** Traffic loss might occur during the restart process.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`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.
Step 4	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays the PIM running-configuration information, including the **flush-routes** command.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Restarting the PIM6 Process

Before you begin

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

SUMMARY STEPS

1. **restart pim6**
2. **configure terminal**
3. **ipv6 pim flush-routes**
4. (Optional) **show running-configuration pim6**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**restart pim6** **Example:** `switch# restart pim6`	Restarts the PIM6 process.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`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	(Optional) **show running-configuration pim6** **Example:** `switch(config)# show running-configuration pim6`	Displays the PIM6 running-configuration information, including the **flush-routes** command.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring BFD for PIM in VRF Mode

Note You can configure Bidirectional Forwarding Detection (BFD) for PIM by either VRF or interface.

Note BFD is not supported for PIM6.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip pim bfd**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**vrf context** *vrf-name*
	Example:
	`switch# vrf context 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 VRF. **Note** You can also enter the **ip pim bfd** command in global configuration mode, which enables BFD on the VRF instance.

Configuring BFD for PIM in Interface Mode

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type*
3. **ip pim bfd instance**
4. (Optional) **show running-configuration pim**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	**ip pim bfd instance** **Example:** `switch(config-if)# ip pim bfd instance`	Enables BFD on the specified interfaces. You can enable or disable BFD on PIM interfaces irrespective of whether BFD is enabled on the VRF.
Step 4	(Optional) **show running-configuration pim** **Example:** `switch(config-if)# show running-configuration pim`	Displays the PIM running-configuration information.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling the Multicast Heavy and Extended Heavy Template

You can enable the multicast heavy template in order to support up to 32K IPv4 mroutes.

You must enable the multicast extended heavy template and configure the multicast route memory in order to support the 128K IPv4 route.

With the heavy template, the **show ip mroute** command displays the multicast traffic counters.

Before you begin

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

Note If the **feature tunnel** command is configured, you must not enable multicast heavy template because the **feature tunnel** command may break the multicast functionality if multicast heavy template is enforced.

SUMMARY STEPS

1. **configure terminal**
2. **system routing** *template-name*
3. **vdc** *vdc-name*
4. **limit-resource m4route-mem** [**minimum** *min-value*]**maximum** *max-value*
5. **exit**
6. **ip routing multicast mfdm-buffer-route-count** *size*
7. **ip pim mtu** *size*
8. **exit**
9. **show system routing mode**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**system routing** *template-name*
	Example:
	`switch(config)# system routing template-multicast-heavy`
	`switch(config)# system routing template-multicast-ext-heavy`
	`switch(config)# system routing template-dual-stack-mcast`
		Enables the multicast template. The template can be template-multicast-heavy or template-multicast-ext-heavy or template-dual-stack-mcast. You need to reload the system after enabling the command when you use template-multicast-heavy or template-multicast-ext-heavy templates.

Step 3	**vdc** *vdc-name* **Example:** `switch(config)# vdc vdc1`	Specifies a VDC and enters VDC configuration mode.
Step 4	**limit-resource m4route-mem** [**minimum** *min-value*]**maximum** *max-value* **Example:** `switch(config-vdc)# limit-resource m4route-mem minimum 150 maximum 150`	Configures IPv4 multicast route map memory resource limits for a VDC. After configuring this command, save it to the startup configuration and reload the device.
Step 5	**exit** **Example:** `switch(config-vdc)# exit`	Exits VDC configuration mode.

	Command or Action	Purpose
Step 6	**ip routing multicast mfdm-buffer-route-count** *size* **Example:** `switch(config)# ip routing multicast mfdm-buffer-route-count 400`	Configures the multicast mfdm buffer route size.
Step 7	**ip pim mtu** *size* **Example:** `switch(config)# ip pim mtu 1500`	Enables bigger frame sizes for the PIM control plane traffic and improves the convergence.
Step 8	**exit** **Example:** `switch(config)# exit`	Exits the global configuration mode.

Step 9	**show system routing mode**
	Example:
	`switch# show system routing mode`
	`Configured System Routing Mode: Multicast Extended Heavy Scale`
	`Applied System Routing Mode: Multicast Extended Heavy Scale`
	`Switch#`
		Displays the configured routing mode - multicast heavy or multicast extended heavy or dual stack.

Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

SG-RouterID Hash

The SG-RouterID Hash feature leverages the Router-IDs to solve the problem of inconsistent hashing in spine-leaf topologies with Equal-Cost Multi-Path (ECMP). Inconsistent hashing leads to inefficient multicast traffic replication and increased resource consumption.

SG-RouterID Hash addresses this by using a consistent Router-ID, ensuring all leaf nodes hash to the same spine nodes for a given multicast flow.

Router-IDs play a crucial role in ensuring consistent multicast traffic distribution across a network. Router-IDs are configured per VRF and advertised in PIM hello messages.

How SG-RouterID Hashing Works

Summary

SG-RouterID Hashing functions like the SG-Next-Hop hash. The key difference is that when a next-hop is a PIM neighbor configured with a Router-ID, the Router-ID is used in the hash computation instead of the next-hop address.

Workflow

SG-RouterID Hashing uses these steps:

1. Router-IDs are configured per VRF.
2. Configured Router-IDs are advertised in PIM hello messages.
3. Using the Interface ID hello option (RFC 6395), both Router IDs and Interface IDs are advertised.

   Each interface has a 32-bit Interface ID derived from the ifIndex.
4. When calculating the hash for a Next-Hop:

When	Then
Next-Hop is a PIM neighbor AND has advertised a Router-ID	Use the Router-ID as input to the SG-Next-Hop hash function instead of the Next-Hop address.
Next-Hop is NOT a PIM neighbor OR has NOT advertised a Router-ID	Use the Next-Hop address as input to the SG-Next-Hop hash function (as usual).

5. When Tie-Breaking with Interface-ID:

When	Then
Multiple best Next-Hops are found	Recalculate the hash using the Interface-ID as a tie-breaker.
Neighbor hasn't advertised an Interface-ID	Use Interface-ID 0 in the hash calculation.

Benefits of SG-RouterID Hash

- **Reduced Replication:** By ensuring consistent hashing across all leaf nodes, the SG-RouterID Hash feature minimizes multicast traffic replication. This means that the same data stream is not unnecessarily duplicated and sent multiple times across the network.
- **Reduced Data Usage:** The reduction in replication directly translates to reduced data usage. Less duplicate traffic is sent, conserving valuable bandwidth resources.
- **Reduced State:** Consistent hashing simplifies the forwarding process, reducing the amount of state information that routers need to maintain. This can improve overall network performance and scalability.

Configure SG-RouterID Hash

This task describes how to configure the SG-RouterID Hash feature to ensure consistent hashing in topologies where multiple leaf nodes share the same ECMP next-hops.

Use these steps to configure the SG-RouterID Hash feature:

Before you begin

Before configuring the SG-RouterID Hash feature, ensure these conditions are met:

- Ensure that your device's software supports the SG-RouterID Hash feature. Once configured, downgrading to a software version that does not support this feature will be blocked.

- Consistent hashing requires consistent ECMP next-hop sets. If receiver leaves lack connectivity to the same set of spines (and therefore don't see the same spines as ECMP next-hops), the leaves might not choose the same spines.
- If leaf nodes have next-hops that are not PIM neighbors, they might not all hash to the same spine.

Procedure

Step 1 Enable SG-RouterID Hash.

Example:

(IPv4)

```
configure terminal
ip multicast multipath sg-routerid
end
```

Example:

(IPv6)

```
configure terminal
ipv6 multicast multipath sg-routerid
end
```

- This command turns on the SG-RouterID hashing in a VRF.
- This command is primarily needed on the leaf nodes in a spine-leaf topology, as the hashing is performed by the leaves.
- Use `no ip[v6] multicast multipath sg-routerid` to disable the feature.

Note
This feature does not apply to NBM and TRM.

Step 2 Configure the Router-ID.

Example:

(IPv4)

```
configure terminal
vrf context <VRF-NAME>
ip pim router-id <ip-address>
end
```

Example:

(IPv6)

```
configure terminal
vrf context <VRF-NAME>
ipv6 pim router-id <ip-address>
end
```

- On each router participating in the SG-RouterID Hash, configure a Router-ID for each VRF.
- Configuring the Router-ID is primarily needed on the spine nodes in a spine-leaf topology, as the leaves use these Router-IDs for hashing.

- For IPv6, this command requires a 32-bit Router-ID, which can be any IPv4 address or identifier.

Step 3 (Optional) Prefer PIM Neighbors

Example:

(IPv4)

```
configure terminal
ip multicast rpf prefer-nbr
end
```

Example:

(IPv6)

```
configure terminal
ipv6 multicast rpf prefer-nbr
end
```

- This command configures the device to prefer PIM neighbors when hashing.
- Use `no ip[v6] multicast rpf prefer-nbr` to disable this behavior.

Verifying SG-RouterID Hash Configuration

Use these commands to verify the SG-RouterID Hash configuration:

Procedure

Step 1 Verify Multipath Configuration

Example:

```
show ip[v6] multicast vrf <VRF-NAME>
```

- This command displays the multipath configuration for the specified VRF.
- Verify that the output shows sg-routerid as the configured multipath hash.

Step 2 Verify PIM Neighbor Information

Example:

```
show ip[v6] pim neighbor internal
```

- This command displays internal PIM neighbor information.
- Check the output for the Router-ID and Interface-ID of each PIM neighbor.
- If the Router-ID was configured on the neighbor, it will be displayed in the output.

Step 3 Verify MRIB PIM Cache.

Example:

```
show routing multicast internal pim-cache
```

- This command displays the MRIB PIM cache information.
- Look for the "IF Database for VRF" section for the relevant VRF.
- Check the "PIM Neighbor" entries for the Router-ID and Interface-ID.
- Example output:

```
Interface: Ethernet1/1, DR: 192.0.2.2,
PIM Neighbor: 192.0.2.1 uptime: 15:50:33
Interface-ID: 0.0.0.1:436208128
```

This verifies that MRIB has learned the correct Router-ID and Interface-ID from PIM.

Verifying the PIM and PIM6 Configuration

To display the PIM and PIM6 configuration 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** [*ip-address*] [**detail** | **summary**]	Displays the IP or IPv6 multicast routing table. The **detail** option displays detailed route attributes. The **summary** option displays route counts and packet rates. **Note** This command also displays multicast counters for Cisco Nexus 9300-EX and 9300-FX Series switches, if the multicast heavy template is enabled. See sample outputs below.
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** [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see the **show ip**[**v6**] **pim rp** command.
show ip[**v6**] **pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays information by the interface.

Command	Description
show ip[**v6**] **pim neighbor** [**interface** *interface* | *ip-prefix*] [**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 outgoing interface (OIF) list.
show ip[**v6**] **pim route** [*source* | *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** [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known to the software, how they were learned, and their group ranges. For similar information, see the **show ip**[**v6**] **pim group-range** command.
Show ip pim vrf *vrf* **detail**	Displays whether PIM graceful SPT switchover feature is up or not.
show ip pim rp-hash *group* [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information.

Command	Description
show ip[**v6**] **pim config-sanity**	

Command	Description
	Displays the following messages if any PIM configuration errors are detected: For Static RPs: • *interface_name* should be PIM enabled • *interface_name* should be UP For Anycast RPs: • Anycast-RP *rp_address* should be configured on local interface • For Anycast-RP *rp_address*, *interface_name* should be PIM enabled • Anycast-RP *rp_address* is not configured as RP for any group-range • *interface_name* should be PIM enabled • *interface_name* should be UP • None of the members in Anycast-RP set for *rp_address* is local For BSR RPs: • BSR RP Candidate interface *interface_name* is not PIM/IP enabled • BSR RP Candidate interface *interface_name* is not IP enabled • BSR RP Candidate interface *interface_name* is not PIM enabled • *interface_name* should be PIM enabled

Command	Description
	• BSR Candidate interface *interface_name* is not PIM/IP enabled • BSR Candidate interface *interface_name* is not IP enabled • BSR Candidate interface *interface_name* is not PIM enabled For Auto-RPs: • Auto-RP RP Candidate interface *interface_name* is not PIM/IP enabled • Auto-RP RP Candidate interface *interface_name* is not IP enabled • Auto-RP RP Candidate interface *interface_name* is not PIM enabled • *interface_name* should be PIM enabled • Auto-RP Candidate interface *interface_name* is not PIM/IP enabled • Auto-RP Candidate interface *interface_name* is not IP enabled • Auto-RP Candidate interface *interface_name* is not PIM enabled
show running-config pim[**6**]	Displays the running-configuration information.
show startup-config pim[**6**]	Displays the startup-configuration information.
show ip[**v6**] **pim vrf** [*vrf-name* | **all**] [**detail**]	Displays per-VRF information.

This example shows sample output, including multicast counters, for the **show ip mroute summary** command:

```
switch# show ip mroute summary
IP Multicast Routing Table for VRF "default"
Route Statistics unavailable - only liveness detected

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
Group count: 700, rough average sources per group: 1.0

Group: 224.1.24.0/32, Source count: 1
Source          packets      bytes           aps   pps       bit-rate     oifs
192.205.38.2    3110         158610          51    0         27.200  bps  5

Group: 224.1.24.1/32, Source count: 1
Source          packets      bytes           aps   pps       bit-rate     oifs
192.205.38.2    3106         158406          51    0         27.200  bps  5
```

This example shows sample output, including multicast counters, for the **show ip mroute** *ip-address* **summary** command:

```
switch# show ip mroute 224.1.24.1 summary
IP Multicast Routing Table for VRF "default"
Route Statistics unavailable - only liveness detected

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
Group count: 700, rough average sources per group: 1.0

Group: 224.1.24.1/32, Source count: 1
Source          packets      bytes           aps   pps       bit-rate     oifs
192.205.38.2    3114         158814          51    0         27.200  bps  5
```

This example shows sample output, including multicast counters, for the **show ip mroute detail** command:

```
switch# show ip mroute detail
IP Multicast Routing Table for VRF "default"

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1

(192.205.38.2/32, 224.1.24.0/32), uptime: 13:03:24, nbm(5) pim(0) ip(0)
  Data Created: No
  Stats: 3122/159222 [Packets/Bytes], 27.200  bps
  Stats: Active Flow
  Incoming interface: Ethernet1/51, uptime: 13:03:24, internal
  Outgoing interface list: (count: 5)
    Ethernet1/39, uptime: 13:03:24, nbm
    Ethernet1/40, uptime: 13:03:24, nbm
    Ethernet1/38, uptime: 13:03:24, nbm
    Ethernet1/37, uptime: 13:03:24, nbm
    Ethernet1/36, uptime: 13:03:24, nbm
```

This example shows sample output, including multicast counters, for the **show ip mroute** *ip-address* **detail** command:

```
switch# show ip mroute 224.1.24.1 detail
IP Multicast Routing Table for VRF "default"
```

```
Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1

(192.205.38.2/32, 224.1.24.1/32), uptime: 13:00:32, nbm(5) ip(0) pim(0)
  Data Created: No
  Stats: 3110/158610 [Packets/Bytes], 27.200  bps
  Stats: Active Flow
  Incoming interface: Ethernet1/50, uptime: 12:59:04, internal
  Outgoing interface list: (count: 5)
    Ethernet1/39, uptime: 12:59:04, nbm
    Ethernet1/40, uptime: 12:59:04, nbm
    Ethernet1/38, uptime: 12:59:04, nbm
    Ethernet1/37, uptime: 12:59:04, nbm
    Ethernet1/36, uptime: 13:00:32, nbm
```

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 these commands.



Note 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*]	Displays global statistics.

Clearing PIM and PIM6 Statistics

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

Command	Description
clear 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** *vrf-name*]	Clears global counters handled by the PIM process.

Null-Register Packing

Beginning with Cisco NX-OS Release 10.5(1)F, you can configure Null-Register packing to send multiple multicast (S, G)s in one Null-Register packet and reduce the packet processing overhead in the PIM routers. This feature is implemented according to RFC 9465.

Configure this feature on the RP and DR because RP and DR are chosen per S, G. The DR periodically sends Null-Registers for each (S,G) to the RP. With this feature, multiple (S, G)s will be packed into one Packed Null-Register and sent to the RP. To enable packing, configuration has to be enabled on both the RP and the DR.

Configuring Null-Register Packing

Execute the following command to configure Null-Register packing. This feature does not use the PIM global MTU if configured.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip pim register-packing [mtu <mtu-size>] [reg-probe-timer <interval>]**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

Step 3	**ip pim register-packing [mtu <mtu-size>] [reg-probe-timer <interval>]**
	Example:
	`switch# ip pim register-packing mtu 1500`
	`switch# ip pim register-packing reg-probe-timer 400`
	`switch# ip pim register-packing mtu 700 reg-probe-timer 400`
		Configures Null-Register packing.
		To simply enable the feature, execute **ip pim register-packing**.
		You can choose to specify either MTU or probe interval, both, or none of them.
		<mtu-size> - default value is 576, value between 576-9216 can be chosen.
		<interval> - default value is 60, value between 60-65535 can be chosen.

Configuring Multicast Service Reflection

The Multicast Service Reflection feature enables you to translate externally received multicast destination addresses to addresses that conform to your organization's internal addressing policy. It is the multicast Network Address Translation (NAT) of an externally received multicast stream (S1,G1) to (S2,G2) into the internal domain. Unlike IP NAT, which only translates the source IP address, the Multicast Service Reflection translates both the source and destination addresses.

The Ingress NAT allows translation of incoming (S,G) into a different source, group or both. All receivers inside the domain then can join the post translated flow. This feature is useful when multicast traffic:

- enters a network from a different domain with potentially overlapping address
- comes with an address that is not understood by applications in the network

The Egress NAT allows translating existing flow (S,G) to different source or group address on a per outgoing interface basis. This feature is useful for multicast distribution to external entities which may only accept a certain source, group address. It can also serve as a way to hide internal address space when flows are exposed to external entities.

The Multicast Service Reflection feature is configured on a loopback interface in the VRF configuration mode. The flow incoming as S1, G1 is translated to S2, G2 and the destination MAC address is re-written to the multicast MAC address of translated address which is G2.

Unicast to Multicast NAT (UM NAT)

Beginning with Cisco NX-OS Release 10.2(2)F, Unicast-to-Multicast NAT (UMNAT) translation is supported. UMNAT is ingress NAT, follows the software design of egress NAT.

For UM NAT, you must configure unicast bandwidth reservation on the port where the pre-translated unicast traffic arrives so that multicast traffic on that port will not consume all the port bandwidth.

Guidelines and Limitations for Multicast Service Reflection

The Multicast Service Reflection feature has the following guidelines and limitations:

- The Multicast Service Reflection feature is introduced in Cisco NX-OS Release 9.3(5) and it is is supported on the Cisco Nexus 9300-FX, FX2, FXP, EX Series switches.
- Beginning with Cisco NX-OS Release 9.3(5)F, the range for maximum replications for the map interface is 1-40.
- Beginning with Cisco NX-OS Release 9.3(3)F, multicast NAT is supported on Cisco Nexus C9300-GX.
- Beginning with Cisco NX-OS Release 10.2(1)F, multicast NAT is supported on Cisco Nexus C9300-GX2B.
- Beginning with Cisco NX-OS Release 10.4(1)F, multicast NAT is supported on Cisco Nexus C9332D-H2R.
- Beginning with Cisco NX-OS Release 10.4(2)F, multicast NAT is supported on Cisco Nexus C93400LD-H1.
- Beginning with Cisco NX-OS Release 10.4(3)F, multicast NAT is supported on Cisco Nexus C9364C-H1 and C9300-FX3.

- Beginning with Cisco NX-OS Release 10.5(2)F, the range for maximum replications for the map interface is increased to 1-250. This enhanced range is supported on all the platforms that support multicast NAT.
  - Downgrading to earlier releases from 10.5(2)F when more than 40 map interfaces are configured, error will occur. To avoid the error, delete service reflection configuration, as well as reduce number of replication interfaces to 40 or bellow, to perform software downgrade.
  - Provisioning 250 replication map interfaces may take up to 3 minutes to be provisioned.
- Beginning with Cisco NX-OS Release 10.1(1)F, Multicast Service Reflection with NBM is supported on Cisco Nexus 9300-FX3, Cisco Nexus C9316D-GX, Cisco Nexus C93600CD-GX, and Cisco Nexus C9364C-GX platform switches.
- The Multicast Service Reflection feature is not supported on the following platforms:
  - Cisco Nexus 9500 series switches with cloud scale line cards
  - Cisco Nexus 9500 series switches with R-series line cards
  - Cisco Nexus 3600-R series switches
  - Cisco Nexus 9200 series switches
  - Cisco Nexus 9364C switches
- Layer2 interfaces are not supported as static OIFs for multicast egress NAT (ENAT). Hence, if you configure a Layer2 interface as static OIF, it would show the interface as inactive in **show ip mroute sr**.
- The Multicast Service Reflection feature is supported in Protocol Independent Multicast (PIM) sparse mode only (ASM or SSM).
- The Multicast Service Reflection feature does not work in a vPC environment.
- Multicast-to-Unicast NAT is supported from Cisco NX-OS Release 10.2(1)F.
- Multicast-to-Unicast NAT translation is supported only in egress mode.
- Multicast-to-Unicast NAT translation is supported on Cisco Nexus 9300-FX, FX2 switches.
- Multicast-to-Unicast translation is not supported in Cisco NX-OS Release 10.1(x).
- PMN supports Multicast-to-Unicast NAT in both PIM active and PIM passive modes.
- From Release 10.2(2)F, Unicast-to-Multicast NAT translation is supported.
- Multicast-to-Multicast and Unicast-to-Unicast NAT configuration cannot be done together and at the same time.
- Unicast NAT, Multicast NAT, and PBR features are not supported at the same time on the same device.
- Egress NAT functionality is supported only under default VRF and not under other VRFs.
- FEX is not supported.
- Multicast Service Reflection feature does not support non-NATed receivers for pre-translated (S1,G1) if a NAT rule is configured for this pair (i.e., ingress NAT does not support the pre-translated (S1,G1) receivers while the egress NAT supports them). The untranslated receiver OIFs are supported for egress NAT.
- SVI is not supported for RPF and OIFs.

- Subinterface receiver for post-translated Egress NAT groups is not supported.
- The selected hardware loopback port for a Multicast Service Reflection configuration should be a physical port with a 'Link Down' state and with no SFP connected.
- The multicast NAT translation does not happen with the mask length 0 to 4. This mask length limitation is only for the group address and it is not for the source addresses.
- Beginning with Cisco NX-OS Release 10.2(1q)F, Multicast NAT is supported on Cisco Nexus N9KC9332D-GX2B platform switches.
- For IGMP static joins on interfaces the group range mask of /24 are used to generate the joins. The source mask length is considered as /32. A variation in source mask length is not considered in generating the joins in the **ip igmp static** join command.
- If you configure **no system multicast dcs-check** and the corresponding (*,G) is present in the switch, the traffic with unknown sources is leaked to the switch.
- If you configure no system multicast dcs check in data-driven SSM traffic, the regular FHR SSM traffic gets leaked to the switch and creates (S,G).

Ingress and egress interface ACLs on a device configured for the Multicast Service Reflection feature have the following limitations:

- When an ingress ACL is applied to block the untranslated multicast traffic that is already flowing, the (S,G) entries are not removed. The reason is that the multicast route entries continue to be hit by the traffic, even though the ACL drops the packets.
- When an egress ACL is applied to block translated source traffic (S2,G2) on an egress interface, the egress ACL does not work because an egress ACL is not supported for the translated traffic.

  Multicast egress NAT is supported in PIM-Passive mode. In PIM-Passive mode, external controller does the bandwidth management for the flows and provisions both pre-translated and post-translated flows.

  For pre-translated flow, controller will call switch Rest API to provision with RPF interface where the pre-translated flow will come in with no OIF.

  For post-translated flow, controller will call switch Rest API to provision with RPF interface same as service-reflect source loopback interface and OIF same as the interface defined in SR rule.

Prerequisites

Multicast Service Reflection feature has the following prerequisite:

For platforms that support the Multicast Service Reflection feature, TCAM needs to be carved before configuring Multicast NAT. Use the following command:

```
hardware access-list tcam region mcast-nat region tcam-size
```

Configuring Multicast Service Reflection

Before you begin

- Make sure your multicast-enabled network runs either Protocol Independent Multicast Sparse Mode (PIM-SM) or PIM Source Specific Multicast (PIM-SSM).

- Make sure that the virtual interface for Multicast Service Reflection is configured in your NAT router and the Multicast Service Reflection rules are configured and operational.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *name*
3. **[no] ip service-reflect source-interface** *interface-name interface-number*
4. **[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*]
5. **[no] ip service-reflect mode egress** *prefix*
6. **[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*] [**static-oif** *out-if*]
7. **[no] multicast service-reflect interface all map interface** *interface-name* **max-replication** *replication*
8. **exit**
9. **interface** *interface-name interface-number*
10. **ip address** *prefix*
11. **ip pim sparse-mode**
12. **ip igmp static-oif** {*group* [**source** *source*] |**route-map** *policy-name*}
13. **no system multicast dcs-check**
14. **ip pim border-router**
15. **nbm external-link**
16. **exit**
17. **[no] multicast service-reflect interface all map interface** *interface-name* **vrf** *vrf-name*
18. **[no] multicast service-reflect interface** *interface-name* **map interface** *interface-name***vrf** *vrf-name*
19. **[no] multicast service-reflect interface** *interface-1, interface-2, interface-3***map interface** *interface-name***vrf** *vrf-name*
20. **exit**
21. **show ip mroute sr**
22. **show forwarding distribution multicast route**
23. **show forwarding distribution multicast route group**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

	Command or Action	Purpose

Step 2	**vrf context** *name*
	Example:
	`switch(config)# vrf context test`
	`switch(config-vrf)#`
		Creates a new VRF and enters VRF configuration mode. The *name* can be any case-sensitive, alphanumeric string up to 32 characters. The NAT rules are configured the vrf context.
		Note
		Non-default VRF is not supported for egress NAT.

Step 3	**[no] ip service-reflect source-interface** *interface-name interface-number* **Example:** `switch(config-vrf)# ip service-reflect source-interface loopback10`	Configures a loopback as the NAT source. This interface pulls traffic to the NAT router. The interface will be RPF for the post translated routes. This command is configured per VRF.
Step 4	**[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*] **Example:** `switch(config-vrf)# ip service-reflect destination 228.1.1.1 to 238.1.1.1 mask-len 32 source 80.80.80.80 to 90.90.90.90 mask-len 32 to-udp-src-port 500 to-udp-dest-port 600`	Configures the NAT rule for the ingress NAT.
Step 5	**[no] ip service-reflect mode egress** *prefix* **Example:** `switch(config-vrf)# ip service-reflect mode egress 225.1.1.0/24`	Configures the egress NAT mode. Matches and rewrites multicast packets routed on to the interface. **Note** Egress NAT is supported only on the default VRF.
Step 6	**[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*] [**static-oif** *out-if*] **Example:** `switch(config-vrf)# ip service-reflect destination 225.1.1.1 to 227.1.1.1 mask-len 32 source 10.10.10.100 to 20.10.10.101 mask-len 32 to-udp-src-port 33 to-udp-dest-port 66 static-oif Ethernet1/8`	Configures the NAT rule for the egress NAT.
Step 7	**[no] multicast service-reflect interface all map interface** *interface-name* **max-replication** *replication* **Example:** `switch(config-vrf)# multicast service-reflect interface all map interface Ethernet1/54 max-replication 3`	Specifies the maximum replications for the map interface. The range is 1–40. Default value is 40. Beginning with Cisco NX-OS Release 10.5(2)F, the range is increased to 1-250. Default value is 40. The **no** command deletes the configuration.

	Command or Action	Purpose

Step 8	**exit**
	Example:
	`switch(config-vrf)# exit`
	`switch(config)#`
		Exits the VRF configuration mode and enters the global configuration mode.

Step 9	**interface** *interface-name interface-number*
	Example:
	`switch(config)# interface loopback10`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 10	**ip address** *prefix* **Example:** `switch(config-if)# ip address 1.1.1.1/24`	Configures an IP address for the loopback interface. It should be a unique IP address that helps to identify this router.
Step 11	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the interface. The default is disabled.
Step 12	**ip igmp static-oif** {*group* [**source** *source*] |**route-map** *policy-name*} **Example:** `switch(config-if)# ip igmp static-oif 230.1.1.1`	Statically binds a multicast group to the outgoing interface, which is handled by the device hardware. If you specify only the group address, the (*, G) state is created. If you specify the source address, the (S, G) state is created. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. Enables the configured loopback interface to join the multicast stream that is to be NATed.
Step 13	**no system multicast dcs-check** **Example:** `switch(config-if)# no system multicast dcs-check`	Enables multicast packets punt to CPU on non-FHR devices for route learning. This is generally used when **ip pim border-router** or **ip igmp host-proxy** features are enabled. This command is not supported on the Cisco Nexus 9300 series and Cisco Nexus 9200 series EOR switches, Cisco Nexus 9504 and Cisco Nexus 9508 EOR and TOR switches, and N3K-C3636C-R, N3K-C36180YC-R TOR switches.
Step 14	**ip pim border-router** **Example:** `switch(config-if)# ip pim border-router`	Ensures that the traffic from sources outside the PIM-SM domain reaches the receivers inside the domain and allows the remotely sourced traffic to reach local receivers in this domain. A PIM Border Router is required when no PIM messages can traverse the PIM domain border.
Step 15	**nbm external-link** **Example:** `switch(config-if)# nbm external-link`	Configures the NBM interface as an external link in order to connect multiple fabrics together in a multisite solution. **Note**

	Command or Action	Purpose
		This command is needed only if feature NBM is enabled and on the links where the **ip pim border-router** command is enabled.

Step 16	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode and enters the global configuration mode.

Step 17	**[no] multicast service-reflect interface all map interface** *interface-name* **vrf** *vrf-name* **Example:** `switch(config)# multicast service-reflect interface all map interface loopback10 vrf test`	Maps all the fan-out interfaces to a service interface. **Note** The **vrf** *vrf-name* option is not supported for egress NAT. **Note** The commands in steps 17, 18, and 19 are needed only in case of Egress NAT. Each OIF used in the Egress NAT rules configuration need to be mapped to one service-interface using one of these mapping configurations.
Step 18	**[no] multicast service-reflect interface** *interface-name* **map interface** *interface-name***vrf** *vrf-name* **Example:** `switch(config)# multicast service-reflect interface ethernet1/18 map interface loopback10 vrf test`	Configures one-to-one mapping of fan-out interface to a service interface.
Step 19	**[no] multicast service-reflect interface** *interface-1, interface-2, interface-3***map interface** *interface-name***vrf** *vrf-name* **Example:** `switch(config)# multicast service-reflect interface ethernet 1/1-10, ethernet1/12-14, ethernet1/16 map interface loopback10 vrf test`	Configures multi-to-one mapping of fan-out interfaces to a service interface.
Step 20	**exit** **Example:** `switch(config)# exit`	Exits the global configuration mode and enters the privileged EXEC mode.
Step 21	**show ip mroute sr** **Example:** `switch# show ip mroute sr`	Displays the service reflection mroute entries.
Step 22	**show forwarding distribution multicast route** **Example:** `switch# show forwarding distribution multicast route`	Displays information about the pre-translated and the post-translated route information for the egress NAT and pre-translated route information for the ingress NAT.

	Command or Action	Purpose
Step 23	**show forwarding distribution multicast route group** **Example:** `switch# show forwarding distribution multicast route group`	Displays information about the multicast FIB distribution IPv4 multicast routes.

Configuration Examples for Multicast Service Reflection

The following example shows the Multicast NAT - ingress and egress configuration:

```
interface loopback0
  ip address 20.1.1.2/24
  ip pim sparse-mode
  ip igmp static-oif 225.1.1.1

hardware access-list tcam region mcast-nat 512

<<Ingress NAT>>

ip route 30.1.1.0/24 10.1.1.1
ip pim ssm range 232.0.0.0/8
ip service-reflect source-interface loopback0
ip service-reflect mode ingress 235.1.1.0/24
ip service-reflect destination 235.1.1.1 to 234.1.1.1 mask-len 32 source 30.1.1.70 to
20.1.1.70 mask-len 32
hardware access-list tcam region mcast-nat 512

<<Egress NAT>>

ip route 30.1.1.0/24 10.1.1.1
ip pim ssm range 232.0.0.0/8
ip service-reflect mode egress 225.1.1.0/24
ip service-reflect destination 225.1.1.1 to 224.1.1.1 mask-len 32 source 30.1.1.1 to 20.1.1.1
 mask-len 32 static-oif port-channel40
ip service-reflect destination 225.1.1.1 to 224.1.1.100 mask-len 32 source 30.1.1.1 to
20.1.1.100 mask-len 32 static-oif port-channel40
ip service-reflect destination 225.1.1.1 to 224.1.1.101 mask-len 32 source 30.1.1.1 to
20.1.1.101 mask-len 32 static-oif port-channel40
ip service-reflect destination 235.1.1.1 to 234.1.1.1 mask-len 32 source 30.1.1.70 to
20.1.1.70 mask-len 32
multicast service-reflect interface all map interface Ethernet1/21
hardware access-list tcam region mcast-nat 512
interface Ethernet1/21
  link loopback
  no shutdown
interface Ethernet1/21.1
  encapsulation dot1q 10
  no shutdown
interface Ethernet1/21.2
  encapsulation dot1q 20
  no shutdown
interface Ethernet1/21.3
  encapsulation dot1q 30
  no shutdown
interface Ethernet1/21.4
  encapsulation dot1q 40
  no shutdown
```

The following examples show the display/output of the Multicast Service Reflection show commands:

```
switch# show ip mroute sr
IP Multicast Routing Table for VRF "default"
(30.1.1.1/32, 225.1.1.1/32), uptime: 01:29:45, ip mrib pim
  NAT Mode: Egress
  NAT Route Type: Pre
  Incoming interface: Ethernet1/1, RPF nbr: 10.1.1.1
  Outgoing interface list: (count: 1)
    loopback0, uptime: 01:29:45, mrib
       SR: (20.1.1.1, 224.1.1.1) OIF: port-channel40
       SR: (20.1.1.100, 224.1.1.100) OIF: port-channel40
       SR: (20.1.1.101, 224.1.1.101) OIF: port-channel40

(30.1.1.70/32, 235.1.1.1/32), uptime: 01:05:12, ip mrib pim
  NAT Mode: Ingress
  NAT Route Type: Pre
  Incoming interface: Ethernet1/1, RPF nbr: 10.1.1.1
  Outgoing interface list: (count: 1)
    loopback0, uptime: 01:05:12, mrib
       SR: (20.1.1.70, 234.1.1.1)
```

```
switch# show ip mroute 234.1.1.1 detail
IP Multicast Routing Table for VRF "default"
Total number of routes: 26
Total number of (*,G) routes: 19
Total number of (S,G) routes: 6
Total number of (*,G-prefix) routes: 1

(20.1.1.70/32, 234.1.1.1/32), uptime: 01:06:30, mrib(0) ip(0) pim(0) static(1)
  RPF-Source: 20.1.1.70 [0/0]
  Data Created: Yes
  Stats: 499/24259 [Packets/Bytes], 27.200  bps
  Stats: Active Flow
  Incoming interface: loopback0, RPF nbr: 20.1.1.70
  LISP dest context id: 0  Outgoing interface list: (count: 1) (bridge-only: 0)
    port-channel40, uptime: 00:59:20, static
```

```
switch# show forwarding distribution multicast route
IPv4 Multicast Routing Table for table-id: 1
Total number of groups: 22
Legend:
   C = Control Route
   D = Drop Route
   G = Local Group (directly connected receivers)
   O = Drop on RPF Fail
   P = Punt to supervisor
   L = SRC behind L3
   d = Decap Route
   Es = Extranet src entry
   Er = Extranet recv entry
   Nf = VPC None-Forwarder
   dm = MVPN Decap Route
   em = MVPN Encap Route
   IPre = Ingress Service-reflect Pre
   EPre = Egress Service-reflect Pre
   Pst = Ingress/Egress Service-reflect Post

  (30.1.1.70/32, 235.1.1.1/32), RPF Interface: Ethernet1/1, flags: IPre
    Upstream Nbr: 10.1.1.1
    Received Packets: 25 Bytes: 1625
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 4
      port-channel40

  (20.1.1.1/32, 224.1.1.1/32), RPF Interface: loopback0, flags: Pst
    Upstream Nbr: 20.1.1.1
```

```
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 2
      port-channel40

  (20.1.1.100/32, 224.1.1.100/32), RPF Interface: loopback0, flags: Pst
    Upstream Nbr: 20.1.1.100
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 2
      port-channel40

  (20.1.1.101/32, 224.1.1.101/32), RPF Interface: loopback0, flags: Pst
    Upstream Nbr: 20.1.1.101
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 2
      port-channel40
```

```
switch# show forwarding multicast route group 235.1.1.1 source 30.1.1.70
slot  1
=======
  (30.1.1.70/32, 235.1.1.1/32), RPF Interface: Ethernet1/1, flags: c
    Received Packets: 18 Bytes: 1170
    Outgoing Interface List Index: 4
    Number of next hops: 1
    oiflist flags: 16384
  Outgoing Interface List Index: 0x4
    port-channel40
```

Unicast to Multicast NAT

Unicast to Multicast NAT works in ingress translation mode. The multicast translated packet can be egress translated back to multicast. The destination address of the unicast packet should match the NAT service reflection interface.

Unicast to Multicast NAT is supported on 1:1 translation. Chain translation, where a multicast to another multicast translation is supported. Multicast to Multicast translation is supported on one to many. For the translation to work, the source IP, the pre and the post must be on the service interface loopback.

The Unicast to Multicast NAT is supported on N9K-C93180YC-FX, N9K-C93180YC2-FX, N9K-C93180YC-FX-24, N9K-C93108TC-FX, N9K-C93108TC2-FX, N9K-C93108TC-FX-24, N9K-C9348GC-F, N9K-C9348GC-FXP, N9K-C9348GC2-FXP, N9K-C9358GY-FXP, N9K-C92348GC, N9K-X9732C-FX, N9K-C9336C-FX2, N9K-C93240YC-FX2, N9K-C93300YC-FX2, N9K-C93240YC-FX2-Z, N9K-C93360YC-FX2, N9K-C93216TC-FX2, N9K-C9336C-FX2-E, N9K-C93180YC-FX3S, N9K-C93180YC-FX3, N9K-C93108TC-FX3P, N9K-C93360YC-FX3, N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C9364C-GX, N9K-C9364D-GX2A, N9K-C9332D-GX2B, N9K-C93560LD-GX2B, and N9K-C9348D-GX2A platforms.

Supported Scales in Unicast to Multicast NAT

Each translation flow requires one ACL to be installed. As this is a 2-pass solution, the service interface bandwidth will determine the limit on number of translations. For a box with only Unicast to Multicast translations, you can scale up to 2047 translations.



Note A setup which has a combination on Unicast to Multicast NAT translations, the maximum number of translations must not exceed 1976.

Egress NAT Platform Recirculation Service Interface

Based on the post translated Multicast group IP, the platform recirculation interface configuration will have the option to select the destination prefix to serve the Unicast to Multicast NAT flow. Based on the bandwidth requirements of each flow, multiple smaller bandwidth flows can share the same recirculation interface. To keep track of the post translated route using the recirculation interfaces, a separate combined database will be maintained for Multicast to Unicast NAT and Unicast to Multicast NAT.

For Unicast to Multicast, the MFDM will pick the parent interface as the service loopback interface so that the same service interface can be shared across multiple routes. The MFDM will overwrite the RPF as the service loopback interface because of the FIB lookup being performed after the packet is recirculated back from the service loopback interface. An ACL is programmed for the Unicast to Multicast NAT with the unicast source IP and destination IP as qualifiers which will drive a redirect_ptr and nat_ptr. The redirect_ptr drives the pact out on the service loopback interface. The nat_ptr translates the source IP, destination IP, and the L4 port information based on the Unicast to Multicast NAT configuration. The redirect_ptr is shared across multiple routes which share the same services loopback interface.

Unicast to Multicast NAT Translations

Unicast to Multicast requires a user to configure source interface where post translated multicast source must fall under source interface subnet. Unicast to multicast translations does not require mode configurations as the incoming traffic is unicast address. The following is the command for configuring source interface:

ip service-reflect source-interface <interface>

The rule configuration takes the unicast address and the multicast address for translation. The following is an example:

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1
mask-len 32 source 21.1.1.1 to 57.1.1.51
mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500
```

MRIB Show commands

The following is the show command for MRIB Unicast to Multicast NAT:

show ip mroute sr umnat

The following are the configurations for Unicast to Multicast NAT:

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1
mask-len 32 source 21.1.1.1 to 57.1.1.51
mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500

ip service-reflect destination 1.2.3.5 to 227.1.1.1
mask-len 32 source 21.1.1.1 to 57.1.1.51
mask-len 32

ip service-reflect destination 227.1.1.1 to 229.1.1.1
mask-len 32 source 57.1.1.51 to 21.1.1.2
mask-len 32 static-oif Ethernet1/7
```

```
switch(config)# show ip mroute sr umnat
IP Multicast Routing Table for VRF "default"
(21.1.1.1/32, 1.2.3.4/32)
Translation:
SR: (57.1.1.51/32, 227.1.1.1/32) udp src: 1000, udp dst : 500
Outgoing interface list: (count: 1)
loopback100, uptime: 1d01h, static
Chained translations:
SR: (21.1.1.2, 229.1.1.1) OIF: Ethernet1/7
(21.1.1.1/32, 1.2.3.5/32)
Translation:
SR: (57.1.1.51/32, 227.1.1.1/32) udp src: 0, udp dst : 0
Outgoing interface list: (count: 1)
loopback100, uptime: 1d01h, static
Chained translations:
SR: (21.1.1.2, 229.1.1.1) OIF: Ethernet1/7
```

MFDM Show Commands

The following is the show command for MFDM Unicast to Multicast NAT:

```
ip service-reflect destination 10.2.3.4 to 239.1.1.1
mask-len 32 source 10.1.1.1 to 8.8.8.8
mask-len 32 to-udp-src-port 10 to-udp-dest-port 20

ip service-reflect destination 10.2.3.5 to 225.1.1.1
mask-len 32 source 10.1.1.2 to 9.9.9.9
mask-len 32
```

```
switch(config)# show forwarding distribution multicast route sr um-nat
(10.1.1.1, 10.2.3.4 -> 8.8.8.8, 239.1.1.1) L4(0,0) SrcIf(Ethernet1/31)
(10.1.1.2, 10.2.3.5 -> 9.9.9.9, 225.1.1.1) L4(0,0) SrcIf(Ethernet1/32)
```

MFIB Show Commands

The following is the show command for MFIB Unicast to Multicast NAT:

```
show forwarding multicast-sr internal-db
Encap 3 (10.1.1.1, 10.2.3.4 -> 8.8.8.8, 239.1.1.1) L4(0,0) SrcIf(Ethernet1/31) Flags(0x0)
Encap 4 (10.1.1.2, 10.2.3.5 -> 9.9.9.9, 225.1.1.1) L4(0,0) SrcIf(Ethernet1/32) Flags(0x0)
```

ACLQOS Show Commands

To display the database for Unicast to Multicast NAT, use the following command:

```
sh system internal aclqos multicast sr hw-to-redir-db <=
Displays ACL hardware index to Redirect index database
```

Unicast to Multicast NAT translation Rule Configuration

The following is the example for Unicast to Multicast NAT translation rule configuration:

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1 mask-len 32 source 21.1.1.1 to 57.1.1.51
 mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500
{
"mribRule": {
"attributes": {
"childAction": "",
"dn":
"sys/mrib/inst/dm-default/sr/rule/pregrp-[1.2.3.4]-postgrp-[227.1.1.1]-gm-32-presrc-[21.1.1.1]-postsrc-[57.1.1.51]-sm-32-srcudp-1000-destudp-500-oif-[unspecified]",
"grpMasklen": "32",
"modTs": "2021-07-24T02:13:54.360+00:00",
"postTransGrp": "227.1.1.1",
```

```
"postTransSrc": "57.1.1.51",
"preTransGrp": "1.2.3.4",
"preTransSrc": "21.1.1.1",
"srcMasklen": "32",
"staticOif": "unspecified",
"status": "",
"udpDestPort": "500",
"udpsrcPort": "1000"
}
}
}
```

Multicast to Unicast NAT

Multicast to unicast NAT is used for hosting content to public cloud. The translation is required as the cloud may not support multicast. After translation, the Unicast packet gets routed as per unicast forwarding logic.

A similar use case is seen when connecting to different sites. If the core does not support multicast end to end, then the content is delivered as unicast to the different sites. The Border box translates multicast to unicast and delivers to different sites for consumption.

For MU NAT, PMN will continue perform bandwidth management for pre-translated multicast flows. For the translated unicast flow, the outgoing interface will need to have unicast bandwidth reservation so that the translated unicast traffic will be sent without any disruption. PMN will also publish the Flow operational MO to indicate the NAT relationship. Since, there are three re-circulations that occur internally for every unicast translation, one must make sure that only one third of the recirculation port bandwidth is assumed. In case of any congestion on the service-reflect map interface used for re-circulation, PMN does not publish a Fault MO.

In PIM Passive mode, Controller will perform Bandwidth management and call Rest APIs to provision the pre-translated flow. PMN will publish the flow operational MO to indicate the NAT relationship.

Examples for MU NAT PIM Passive

The following are the MUNAT Rest API calls and Payload information:

Configure Re-circ Interfaces

```
url: 172.28.249.173/api/mo/sys/mca/config/natsr/mappings.json?rsp-subtree=full
Payload:
{
"mcaNatMapDestPrefixSif": {
"attributes": {
"destPrefix": "112.10.3.0/24",
"domName": "default",
"maxEnatReplications": "40",
"siIfName": "eth1/15",
"status": ""
}
}
}
```

Service Reflect Rules

```
url: <ip_switch>/api/mo/sys/mrib/inst/dom-default/sr/rule.json?rsp-subtree=full
Payload:
{
"mribRule": {
"attributes": {
"grpMasklen": "32",
"postTransGrp": "112.3.3.51",
```

```
"postTransSrc": "11.1.1.3",
"preTransGrp": "225.10.1.50",
"preTransSrc": "112.3.1.2",
"srcMasklen": "32",
"staticOif": "unspecified",
"status": "",
"udpDestPort": "0",
"udpsrcPort": "0"
}
}
}
```

NBM Flows

```
url: <ip_switch>/api/mo/sys/nbm/show/flows/dom-default.json?rsp-subtree=full
Payload:
{
"nbmConfFlow": {
"attributes": {
"bwKbps": "50000",
"group": "225.1.1.1",
"ingressIf": "eth1/2",
"policer": "ENABLED",
"source": "112.3.1.2",
"status": ""
}
}
}
```

Configuration Examples for PIM

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

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

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

4. Configure message filtering.

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

The following example shows how to configure PIM SSM mode:

```
configure terminal
  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
```

PIM SSM Over vPC Configuration Example

This example shows how to override the default SSM range of 232.0.0.0/8 to 225.1.1.0/24. PIM SSM over vPC will work as long as S,G joins are received in this range.

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim ssm range 225.1.1.0/24
switch(config-vrf)# show ip pim group-range --> Shows the configured SSM group range.
PIM Group-Range Configuration for VRF "Enterprise"
Group-range        Mode      RP-address       Shared-tree-only range
225.1.1.0/24       SSM       -                -

switch1# show vpc (primary vPC) --> Shows vPC-related information.
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1000 up     101-102

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
1    Po1    up     success     success                    102
```

```
2    Po2    up     success     success                    101

switch2# show vpc (secondary vPC)
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1000 up     101-102

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
1    Po1    up     success     success                    102

2    Po2    up     success     success                    101


switch1# show ip igmp snooping group vlan 101 (primary vPC IGMP snooping states) --> Shows
 if S,G v3 joins are received and on which VLAN. The same VLAN should be OIF in the MRIB
output.

Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan  Group Address      Ver  Type  Port list
101   */*                -    R     Po1000 Vlan101
101   225.1.1.1          v3
        100.6.160.20           D     Po2

switch2# show ip igmp snooping group vlan 101 (secondary vPC IGMP snooping states)
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan  Group Address      Ver  Type  Port list
101   */*                -    R     Po1000 Vlan101
101   225.1.1.1          v3
        100.6.160.20           D     Po2


switch1# show ip pim route (primary vPC PIM route) --> Shows the route information in the
PIM protocol.
PIM Routing Table for VRF "default" - 3 entries

(10.6.159.20/32, 225.1.1.1/32), expires 00:02:37
  Incoming interface: Ethernet1/19, RPF nbr 10.6.159.20
  Oif-list:       (1) 00000000, timeout-list: (0) 00000000
  Immediate-list: (1) 00000000, timeout-list: (0) 00000000
```

```
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 2, JP-holdtime round-up: 3

(100.6.160.20/32, 225.1.1.1/32), expires 00:01:19
  Incoming interface: Vlan102, RPF nbr 100.6.160.20
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 2, JP-holdtime round-up: 3

(*, 232.0.0.0/8), expires 00:01:19
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 2, JP-holdtime round-up: 3

switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:51
  Incoming interface: Vlan102, RPF nbr 100.6.160.100
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3

(100.6.160.20/32, 225.1.1.1/32), expires 00:02:51
  Incoming interface: Vlan102, RPF nbr 100.6.160.20
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3

(*, 232.0.0.0/8), expires 00:02:51
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3

switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries

(10.6.159.20/32, 225.1.1.1/32), expires 00:02:29
  Incoming interface: Vlan102, RPF nbr 100.6.160.100
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3

(100.6.160.20/32, 225.1.1.1/32), expires 00:02:29
  Incoming interface: Vlan102, RPF nbr 100.6.160.20
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3

(*, 232.0.0.0/8), expires 00:02:29
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3
```

```
switch1# show ip mroute (primary vPC MRIB route) --> Shows the IP multicast routing table.

IP Multicast Routing Table for VRF "default"

(10.6.159.20/32, 225.1.1.1/32), uptime: 03:16:40, pim ip
  Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
  Outgoing interface list: (count: 1)
    Vlan102, uptime: 03:16:40, pim

(100.6.160.20/32, 225.1.1.1/32), uptime: 03:48:57, igmp ip pim
  Incoming interface: Vlan102, RPF nbr: 100.6.160.20
  Outgoing interface list: (count: 1)
    Vlan101, uptime: 03:48:57, igmp

(*, 232.0.0.0/8), uptime: 6d06h, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)

switch1# show ip mroute detail (primary vPC MRIB route) --> Shows if the (S,G) entries have
 the RPF as the interface toward the source and no *,G states are maintained for the SSM
group range in the MRIB.

IP Multicast Routing Table for VRF "default"

Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1

(10.6.159.20/32, 225.1.1.1/32), uptime: 03:24:28, pim(1) ip(0)
  Data Created: Yes
  VPC Flags
    RPF-Source Forwarder
  Stats: 1/51 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
  Outgoing interface list: (count: 1)
    Vlan102, uptime: 03:24:28, pim

(100.6.160.20/32, 225.1.1.1/32), uptime: 03:56:45, igmp(1) ip(0) pim(0)
  Data Created: Yes
  VPC Flags
    RPF-Source Forwarder
  Stats: 1/51 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Vlan102, RPF nbr: 100.6.160.20
  Outgoing interface list: (count: 1)
    Vlan101, uptime: 03:56:45, igmp (vpc-svi)

(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
  Data Created: No
  Stats: 0/0 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)

switch2# show ip mroute detail (secondary vPC MRIB route)
IP Multicast Routing Table for VRF "default"

Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1
```

```
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:26:24, igmp(1) pim(0) ip(0)
  Data Created: Yes
  Stats: 1/51 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Vlan102, RPF nbr: 100.6.160.100
  Outgoing interface list: (count: 1)
    Ethernet1/17, uptime: 03:26:24, igmp

(100.6.160.20/32, 225.1.1.1/32), uptime: 04:06:32, igmp(1) ip(0) pim(0)
  Data Created: Yes
  VPC Flags
    RPF-Source Forwarder
  Stats: 1/51 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Vlan102, RPF nbr: 100.6.160.20
  Outgoing interface list: (count: 1)
    Vlan101, uptime: 04:03:24, igmp (vpc-svi)

(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
  Data Created: No
  Stats: 0/0 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)
```

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# configure terminal
   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# configure terminal
   switch(config)# ip pim bsr forward listen
   ```

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

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

5. Configure message filtering.

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

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

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

5. Configure message filtering.

   ```
   switch# configure terminal
   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:

```
configure terminal
  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# configure terminal
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# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.3/32
switch(config-if)# ip pim sparse-mode
```

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# configure terminal
switch(config)# interface loopback 1
switch(config-if)# ip address 192.0.2.31/32
switch(config-if)# ip pim sparse-mode
```

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

The following example shows how to configure PIM Anycast RP for IPv6:

```
configure terminal
interface loopback 0
ipv6 address 2001:0db8:0:abcd::5/32
ipv6 pim sparse-mode
ipv6 router ospfv3 1 area 0.0.0.0
exit
interface loopback 1
ipv6 address 2001:0db8:0:abcd::1111/32
ipv6 pim sparse-mode
ipv6 router ospfv3 1 area 0.0.0.0
exit
ipv6 pim rp-address 2001:0db8:0:abcd::1111 group-list ff1e:abcd:def1::0/24
ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111
```

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

```
configure terminal
interface ethernet 2/1
ip pim sparse-mode
exit
interface loopback 0
ip address 192.0.2.3/32
ip pim sparse-mode
exit
interface loopback 1
ip address 192.0.2.31/32
ip pim sparse-mode
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
```

PFM-SD Configuration Example

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

1. Configure PFM-SD range on all the switches that have PFM-SD feature enabled.

   ```
   switch(config)# ip pim pfm-sd range 224.0.0.0/4
   ```

2. Configure PFM-SD originator only on FHR.

   ```
   switch(config)# ip pim pfm-sd originator-id loopback0
   ```

3. Configure PFM-SD announcement interval (optional)

   ```
   switch(config)# ip pim pfm-sd announcement interval 100
   ```

4. Configure PFM-SD announcement gap (optional)

   ```
   switch(config)# ip pim pfm-sd announcement gap 1200
   ```

5. Configure PFM-SD announcement rate (optional).

   ```
   switch(config)# ip pim pfm-sd announcement rate 10
   ```

6. Configure PFM_SD gsh holdtime (optional).

   ```
   switch(config)# ip pim pfm-sd gsh holdtime 60
   ```

7. Configure PFM-SD boundary on eth1/2 with the following required option for blocking PFM-SD traffic:
   - **in**: To block incoming PFM-SD traffic
   - **out**: To block outgoing PFM-SD traffic
   - **both**: to block both incoming and outgoing PFM-SD traffic

   ```
   switch(config)# interface ethernet1/2
   switch(config-if)# ip pim pfm-sd boundary in
   ```

The following example shows sample output for the **show run pim** command:

```
switch(config-if)# show run pim

!Command: show running-config pim
!Running configuration last done at: Mon Dec  5 09:01:34 2022
```

```
!Time: Mon Dec  5 09:01:40 2022

version 10.3(2) Bios:version 07.69
feature pim

ip pim prune-on-expiry
ip pim pfm-sd range 224.0.0.0/4
ip pim pfm-sd originator-id loopback0
ip pim pfm-sd announcement interval 100
ip pim pfm-sd announcement gap 1200
ip pim pfm-sd announcement rate 10
ip pim pfm-sd gsh holdtime 60
interface Ethernet1/2
ip pim pfm-sd boundary in
```

The following example shows sample output for the **show ip pim pfm-sd cache** command:

```
switch# show ip pim pfm-sd cache
Legend * - Originator down
PIM PFM Local Cache-Info - VRF "default"
Group: 224.0.0.0, Source count: 1
Source     Originator     Last announced     Holdtime
1.21.21.2  55.55.55.55    00:00:44           00:07:58
```

The following example shows sample output for the **show ip pim pfm-sd cache remote-discovery** command:

```
switch# show ip pim pfm-sd cache remote-discovery
PIM PFM Remote Discovery Cache-Info - VRF "default"
Group: 224.0.0.0, Source count: 1
Source     Originator     Last announced     Holdtime
1.21.21.2  55.55.55.55    00:00:44           00:07:58
```

The following example shows sample output for the **show ip pim vrf internal** command:

```
switch# show ip pim vrf internal
PIM Enabled VRFs
VRF Name     VRF   Table       Interface   BFD         MVPN
             ID    ID          Count       Enabled     Enabled
default      1     0x00000001  8          no          no
PIM RP change: no
…..
PIM VxLAN VNI ID: 0
PIM pfm-sd : Enabled
group range : 224.0.0.0/4
originator interface : loopback0
originator ip : 55.55.55.55
announcement interval : 100 seconds
announcement gap : 1200 milliseconds
announcement rate : 10
holdtime : 60 seconds
```

The following example shows sample output for the **show ip pim interface interface port** command:

```
switch# show ip pim interface ethernet 1/17
PIM Interface Status for VRF "default"
Ethernet1/17, Interface status: protocol-up/link-up/admin-up
IP address: 17.17.17.1, IP subnet: 17.17.17.0/24
……
PIM border-router interface: no
PIM pfm-sd boundary: none
pfm-sd packets sent : 0
pfm-sd packets received :1
pfm-sd packets forwarded :1
```

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 172.21.0.11 prefix-list plist11
ip pim rp-address 172.21.0.22 prefix-list plist22
ip pim rp-address 172.21.0.33 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 172.21.0.11 route-map rmap11
ip pim rp-address 172.21.0.22 route-map rmap22
ip pim rp-address 172.21.0.33 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: 172.21.0.11, (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: 172.21.0.22, (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: 172.21.0.33, (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: 10.165.20.1
  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: 10.165.20.1
  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: 10.165.20.1
  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: 10.0.0.1
  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: 10.0.0.1
  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        ASM       -                -
231.0.0.0/8        ASM       172.21.0.11      -
231.128.0.0/9      ASM       172.21.0.22      -
231.129.0.0/16     ASM       172.21.0.33      -
231.129.128.0/17   Unknown   -                -
```

Tech-support Command

Execute the following command to collect hardware table dump.

SUMMARY STEPS

1. **show tech-support forwarding multicast detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show tech-support forwarding multicast detail**	Collects hardware table dump.

Example

```
show tech-support forwarding multicast hardware module 1
Module:1 Unit:0 Slice: 0 Table:tah_ara_lub_bdstatetable     <<<<<<
ENTRY: 1
        info_leaf_flood_dst_ptr : 0x00000001
        info_leaf_igmp_mld_dst_ptr : 0x00001002
        info_leaf_fid : 0x00000001
        info_leaf_vrf : 0x00000001
……
Module:1 Unit:0 Slice: 0 Table:tah_ara_qsmt_dhs_met_access     <<<<<<
ENTRY: 1
        met_entry_bridge_only : 0x00000001
        met_entry_no_prune_on_mct : 0x00000001
……
```

Related Documents

Related Topic	Document Title
ACL TCAM regions	*Cisco Nexus 9000 Series NX-OS Security Configuration G*
Configuring VRFs	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configu*

Standards

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

MIBs

MIBs	MIBs Link
MIBs related to PIM	To locate and download supported MIBs, go to the follow https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html