Configuring PIM

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

This chapter includes the following sections:

- Information About PIM, page 25
- Licensing Requirements for PIM, page 32
- Guidelines and Limitations for PIM, page 32
- Default Settings, page 33
- Configuring PIM, page 34
- Verifying the PIM Configuration, page 57
- Displaying Statistics, page 58
- Configuration Examples for PIM, page 59
- Where to Go Next, page 62
- Additional References, page 62

Information About PIM

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees on which packets from multiple sources are forwarded, as well as source distribution trees on which packets from a single source are forwarded. For more information about multicast, see the "Information About Multicast" section on page 1-1.

Cisco NX-OS supports PIM sparse mode for IPv4 networks (PIM). (In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it.) You can configure PIM to run simultaneously on a router. You can use PIM global parameters to configure rendezvous points (RPs), message packet filtering, and statistics. You can use PIM interface parameters to enable multicast, identify PIM borders, set the PIM hello message interval, and set the designated router (DR) priority. For more information, see the "Configuring PIM Sparse Mode" section on page 3-36.

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

In Cisco NX-OS, multicast is enabled only after you enable the PIM feature on each router and then enable PIM sparse mode on each interface that you want to participate in multicast. You can configure PIM for an IPv4 network. In an IPv4 network, if you have not already enabled IGMP on the router, PIM enables it automatically. For information about configuring IGMP, see Chapter 2, "Configuring IGMP".

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

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

You can combine the modes to cover different ranges of group addresses. For more information, see the "Configuring PIM" section on page 3-34.

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

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

Note Multicast equal-cost multipathing (ECMP) is on by default in the Cisco NX-OS for the Cisco Nexus 5500 switches; you cannot turn ECMP off. If multiple paths exist for a prefix, PIM selects the path with the lowest administrative distance in the routing table. Cisco NX-OS supports up to 16 paths to a destination.

This section includes the following topics:

- Hello Messages, page 26
- Join-Prune Messages, page 27
- State Refreshes, page 28
- Rendezvous Points, page 28
- PIM Register Messages, page 31
- Designated Routers, page 31
- Administratively Scoped IP Multicast, page 31
- PIM and Virtual Port Channels, page 32

Hello Messages

The PIM process begins when the router establishes PIM neighbor adjacencies by sending PIM hello messages to the multicast address 224.0.0.13. Hello messages are sent periodically at the interval of 30 seconds. When all neighbors have replied, then 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.

Caution If you change the PIM hello interval to a lower value, we recommend that you ensure it is appropriate for your network environment.

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 switch detects a PIM failure on that link.

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

Note If PIM is disabled on the switch, the IGMP snooping software processes the PIM hello messages.

For information about configuring hello message authentication, see the "Configuring PIM Sparse Mode" section on page 3-36.

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 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 mode. SSM does not use an RP but builds a shortest path tree (SPT) that is the lowest cost path between the source and the receiver.

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

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

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

Join-prune messages are sent as quickly as possible by the software. You can filter the join-prune messages by defining a routing policy. For information about configuring the join-prune message policy, see the "Configuring PIM Sparse Mode" section on page 3-36.

You can prebuild the SPT for all known (S,G) in the routing table by triggering PIM joins upstream. To prebuild the SPT for all known (S,G)s in the routing table by triggering PIM joins upstream, even in the absence of any receivers, use the **ip pim pre-build-spt** command. By default, PIM (S,G) joins are triggered upstream only if the OIF-list for the (S,G) is not empty. It is useful in certain scenarios—for example, on the virtual port-channel (vPC) nonforwarding router—to prebuild the SPTs and maintain the (S,G) states even when the system is not forwarding on these routes. Prebuilding the SPT ensures faster convergence when a vPC failover occurs. When you are running virtual port channels (vPCs), enabling this feature causes both vPC peer switches to join the SPT, even though only one vPC peer switch actually routes the multicast traffic into the vPC domain. This behavior results in the multicast traffic passing over two parallel paths from the source to the vPC switch pair, consuming bandwidth on both paths. Additionally, when both vPC peer switches join the SPT, one or more upstream switches in the network may be required to perform additional multicast replications to deliver the traffic on both parallel paths toward the receivers in the vPC domain.

State Refreshes

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

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

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

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

Rendezvous Points

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

This section includes the following topics:

- Static RP, page 28
- BSRs, page 28
- Auto-RP, page 29
- Anycast-RP, page 30

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 switch

For information about configuring static RPs, see the "Configuring Static RPs" section on page 3-40.

BSRs

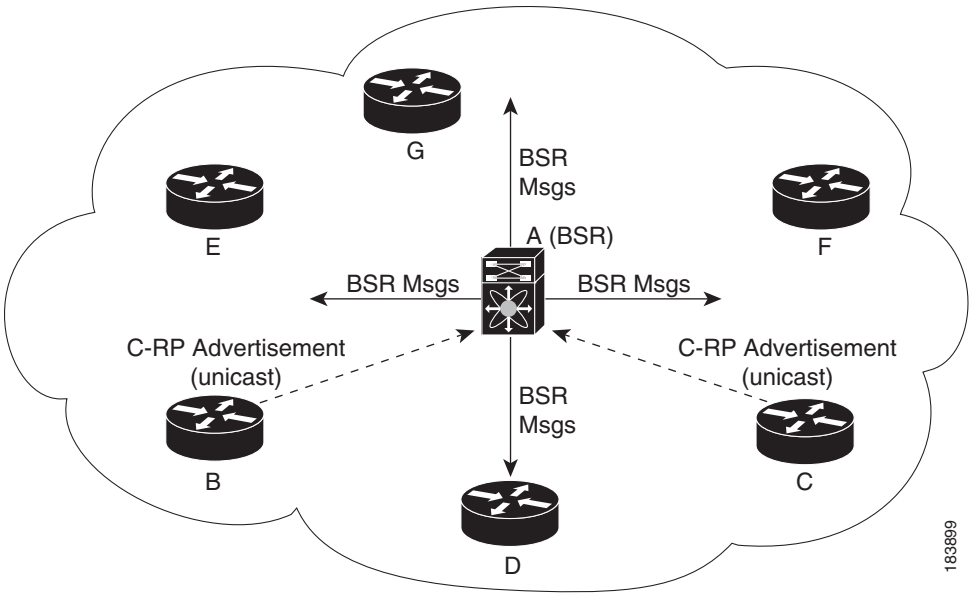
The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs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

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

Figure 3-1 shows where 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 3-1 BSR Mechanism



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

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

For more information about bootstrap routers, see RFC 5059.

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

For information about configuring BSRs and candidate RPs, see the "Configuring BSRs" section on page 3-41.

Auto-RP

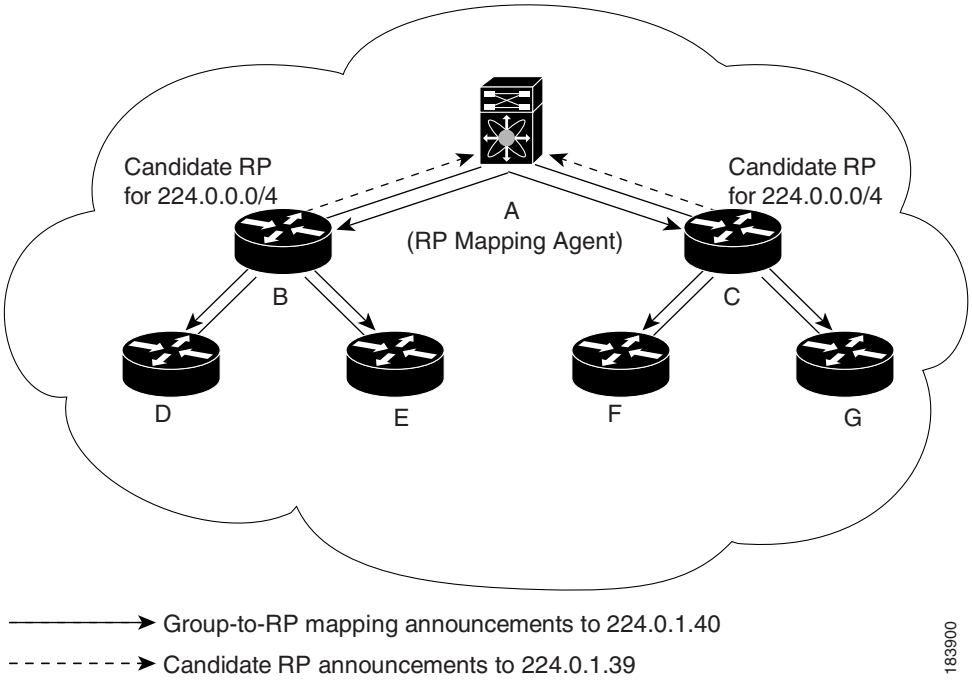
Auto-RP is a Cisco protocol that was prior to the Internet standard bootstrap router mechanism. You configure Auto-RP by selecting candidate mapping agents and RPs. Candidate RPs send their supported group range in RP-Announce messages to the Cisco RP-Announce multicast group 224.0.1.39. An

Auto-RP mapping agent listens for RP-Announce messages from candidate RPs and forms a Group-to-RP mapping table. The mapping agent multicasts the Group-to-RP mapping table in RP-Discovery messages to the Cisco RP-Discovery multicast group 224.0.1.40.

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

Figure 3-2 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 3-2 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.

For information about configuring Auto-RP, see the "Configuring Auto-RP" section on page 3-44.

Anycast-RP

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

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

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

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

For information about configuring Anycast-RPs, see the "Configuring a PIM Anycast-RP Set" section on page 3-46.

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.

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

You can filter PIM register messages by defining a routing policy. For information about configuring the PIM register message policy, see the "Configuring Shared Trees Only for ASM" section on page 3-47.

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" section on page 3-26.

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

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

For information about configuring the DR priority, see the "Configuring PIM Sparse Mode" section on page 3-36.

Administratively Scoped IP Multicast

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

You can configure an interface as a PIM boundary so that PIM messages are not sent out that interface. For information about configuring the domain border parameter, see the "Configuring PIM Sparse Mode" section on page 3-36.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value. For more information, see the "Configuring Shared Trees Only for ASM" section on page 3-47.

Virtualization Support

You can define multiple virtual routing and forwarding (VRF) instances. For each VRF, independent multicast system resources are maintained, including the MRIB.

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

For information about configuring VRFs, see the *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.0*.

PIM and Virtual Port Channels

When a PIM hello message is received by the vPC peer link on a non-vPC port, the vPC peer link on the switch acts as an output interface (OIF) for a multicast group or router port and floods the packet on the vPC peer link, vPC links, and non-vPC links. The peer vPC switch that receives this packet on the vPC peer link floods it on all non-vPC links and adds the peer link to the router port list.

When a PIM hello message is received by the vPC peer link on a vPC port, the vPC port acts as the router port list and the switch floods the packet on the vPC link, vPC peer link, and non-vPC links using Cisco Fabric Services (CFS), which means the packets are encapsulated as CFS packets and sent over the vPC peer link. The peer vPC switch that receives this packet on the vPC peer link will flood it on all non-vPC links and adds the vPC port to the router port list. If, however, the vPC port is down, the PIM software on the switch forwards the packet to the vPC peer link and the peer vPC switch then forwards the packets to all VLANs.

If switch virtual interfaces (SVIs) are enabled on the VLANs of the vPC peers, each vPC peer will act as a designated router (DR) to forward the multicast traffic. If the vPC peer link fails, the SVIs and vPC peer links on the vPC secondary switch also goes down. The primary vPC switch will then forward all multicast traffic.

Licensing Requirements for PIM

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	PIM require a LAN Base Services license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for PIM

PIM has the following guidelines and limitations:

- Cisco NX-OS PIM does not interoperate with any version of PIM dense mode or PIM sparse mode version 1.
- Do not configure both Auto-RP and BSR protocols in the same network.
- Configure candidate RP intervals to a minimum of 15 seconds.
- If a switch is configured with a BSR policy that should prevent it from being elected as the BSR, the switch ignores the policy. This behavior results in the following undesirable conditions:
  - If a switch receives a BSM that is permitted by the policy, the switch, which incorrectly elected itself as the BSR, drops that BSM so that routers downstream fail to receive it. Downstream switches correctly filter the BSM from the incorrect BSR so that they do not receive RP information.
  - A BSM received by a BSR from a different switch sends a new BSM but ensures that downstream switches do not receive the correct BSM.
- A vPC peer link is a valid link for IGMP multicast forwarding.
- If the vPC link on a switch is configured as an output interface (OIF) for a multicast group or router port, the vPC link on the peer switch must also be configured as an output interface for a multicast group or router port.
- In SVI VLANs, the vPC peers must have the multicast forwarding state configured for the vPC VLANs to forward multicast traffic directly through the vPC link instead of the peer link.
- If vPC is enabled, PIM SSM is not supported on the switches.
- A topology that has a PIM router connected to a pair of Cisco Nexus 5500 Platform switches through vPC is not supported.
- Cisco Nexus 5000 series devices do not support per route packet counters. Hence the **show ip mroute summary** command and **show forwarding distribution multicast route group** command do not show correct count of packets sent out. The packets per second (pps) count is shown as zero.
- If you configure the **vpc bind-vrf** command to forward multicast traffic over the vPC peer link, you need to reload the switches to avoid any traffic loss.

Default Settings

Table 3-1 lists the default settings for PIM parameters.

Table 3-1 Default PIM Parameters

Parameters	Default
Use shared trees only	Disabled
Flush routes on restart	Disabled
Log Neighbor changes	Disabled
Auto-RP message action	Disabled
BSR message action	Disabled
SSM multicast group range or policy	232.0.0.0/8 for IPv4
PIM sparse mode	Disabled
Designated router priority	0
Hello authentication mode	Disabled

Table 3-1 Default PIM Parameters (continued)

Parameters	Default
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

Configuring PIM

You can configure PIM for each interface.

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 domain using the multicast distribution modes described in Table 3-2.

Table 3-2 PIM Multicast Distribution Modes

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

To configure PIM, follow these steps:

Step 1 From the multicast distribution modes described in Table 3-2, select the range of multicast groups that you want to configure in each mode.

Step 2 Enable the PIM features. See the "Enabling the PIM Features" section on page 3-35.

Step 3 Configure PIM sparse mode on each interface that you want to participate in a PIM domain. See the "Configuring PIM Sparse Mode" section on page 3-36.

Step 4 Follow the configuration steps for the multicast distribution modes that you selected in Step 1 as follows:

- For ASM mode, see the "Configuring ASM" section on page 3-40.
- For SSM mode, see the "Configuring SSM" section on page 3-48.

- For RPF routes for multicast, see the "Configuring RPF Routes for Multicast" section on page 3-50.

Step 5 Configure message filtering. See the "Configuring Message Filtering" section on page 3-52.

Step 6 Bind VRF. See the "Binding VRFs to vPCs" section on page 3-55.

This section includes the following topics:

- Enabling the PIM Features, page 35
- Configuring PIM Sparse Mode, page 36
- Configuring ASM, page 40
- Configuring SSM, page 48
- Configuring RPF Routes for Multicast, page 50
- Configuring Route Maps to Control RP Information Distribution, page 51
- Configuring Message Filtering, page 52
- Binding VRFs to vPCs, page 55
- Restarting the PIM Processes, page 56

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

Enabling the PIM Features

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

BEFORE YOU BEGIN

Ensure that you have installed the LAN Base Services license.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**feature pim** **Example:** switch(config)# feature pim	Enables PIM. By default, PIM is disabled.
Step 3	**show running-configuration pim** **Example:** switch(config)# show running-configuration pim	(Optional) Shows the running-configuration information for PIM, including the **feature** command.
Step 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

Configuring PIM Sparse Mode

You configure PIM sparse mode on every switch interface that you want to participate in a sparse mode domain. You can configure the sparse mode parameters described in Table 3-3.

Table 3-3 PIM Sparse Mode Parameters

Parameter	Description
Global to the switch	
Auto-RP message action	Enables listening and forwarding of Auto-RP messages. The default is disabled, which means that the router does not listen or forward Auto-RP messages unless it is configured as a candidate RP or mapping agent.
BSR message action	Enables listening and forwarding of BSR messages. The default is disabled, which means that the router does not listen or forward BSR messages unless it is configured as a candidate RP or BSR candidate.
Register rate limit	Configures the IPv4 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 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 switch interface	
PIM sparse mode	Enables PIM on an interface.

Table 3-3 PIM Sparse Mode Parameters (continued)

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.
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.
Hello interval	Configures the interval at which hello messages are sent in milliseconds. The range is from 1 to 4294967295. The default is 30000.
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.
Neighbor policy	Configures which PIM neighbors to become adjacent to based on a route-map policy[1] where you can specify IP addresses to become adjacent to with the **match ip address** command. If the policy name does not exist, or no IP addresses are configured in a policy, then adjacency is established with all neighbors. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator.

1. To configure route-map policies, see the *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.0*.

For information about configuring multicast route maps, see the "Configuring Route Maps to Control RP Information Distribution" section on page 3-51.

Note To configure the join-prune policy, see the "Configuring Message Filtering" section on page 3-52.

BEFORE YOU BEGIN

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

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) **show ip pim rp** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. (Optional) **ip pim register-rate-limit** *rate*
6. (Optional) [**ip** | **ipv4**] **routing multicast holddown** *holddown-period*
7. (Optional) **show running-configuration pim**
8. **interface** *interface*
9. **no switchport**
10. **ip pim sparse-mode**
11. (Optional) **ip pim dr-priority** *priority*
12. (Optional) **ip pim hello-authentication ah-md5** *auth-key*
13. (Optional) **ip pim hello-interval** *interval*
14. (Optional) **ip pim border**
15. (Optional) **ip pim neighbor-policy** *policy-name*
16. (Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]
17. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]} **Example:** switch(config)# ip pim auto-rp listen	(Optional) Enables listening or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen to or forward Auto-RP messages.
Step 3	**ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} **Example:** switch(config)# ip pim bsr forward	(Optional) Enables listening or forwarding of BSR messages. The default is disabled, which means that the software does not listen or forward BSR messages.
Step 4	**show ip pim rp** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** switch(config)# show ip pim rp	(Optional) Displays PIM RP information, including Auto-RP and BSR listen and forward states.

	Command	Purpose
Step 5	**ip pim register-rate-limit** *rate* **Example:** `switch(config)# ip pim register-rate-limit 1000`	(Optional) Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 6	[**ip** | **ipv4**] **routing multicast holddown** *holddown-period* **Example:** `switch(config)# ip routing multicast holddown 100`	(Optional) Configures the initial holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 7	**show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	(Optional) Displays PIM running-configuration information, including the register rate limit.

Step 8	**interface** *interface*
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as **ethernet** *slot/port*.
		
		Note If this is a QSFP+ GEM, the *slot/port* syntax is *slot/QSFP-module/port*.

Step 9	`no switchport`
	
	Example:
	`switch(config-if)# no switchport`
		Configures the interface as a Layer 3 routed interface.

Step 10	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 11	**ip pim dr-priority** *priority* **Example:** `switch(config-if)# ip pim dr-priority 192`	(Optional) Sets the designated router (DR) priority that is advertised in PIM hello messages. Values range from 1 to 4294967295. The default is 1.
Step 12	**ip pim hello-authentication ah-md5** *auth-key* **Example:** `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	(Optional) Enables an MD5 hash authentication key in PIM hello messages. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The key can be up to 16 characters. The default is disabled.
Step 13	**ip pim hello-interval** *interval* **Example:** `switch(config-if)# ip pim hello-interval 25000`	(Optional) Configures the interval at which hello messages are sent in milliseconds. The range is from 1 to 4294967295. The default is 30000. **Note** We do not support aggressive values for the hello interval; any value less than 3000 milliseconds is an aggressive hello-interval value.

	Command	Purpose
Step 14	**ip pim border** **Example:** `switch(config-if)# ip pim border`	(Optional) Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Step 15	**ip pim neighbor-policy** *policy-name* **Example:** `switch(config-if)# ip pim neighbor-policy my_neighbor_policy`	(Optional) Configures which PIM neighbors to become adjacent to based on a route-map policy with the **match ip address** command. The policy name can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator.
Step 16	**show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	(Optional) Displays PIM interface information.
Step 17	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring ASM

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

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

This section includes the following topics:

- Configuring Static RPs, page 40
- Configuring BSRs, page 41
- Configuring Auto-RP, page 44
- Configuring a PIM Anycast-RP Set, page 46
- Configuring Shared Trees Only for ASM, page 47

Configuring Static RPs

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

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

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

Step 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **route-map** *policy-name*] **Example:** `switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`	Configures a PIM static RP address for a multicast group range. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The default mode is ASM. The default group range is 224.0.0.0 through 239.255.255.255. The example configures PIM ASM mode for the specified group range.
Step 3	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM modes and group ranges.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

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 Table 3-4.

Table 3-4 Candidate BSR Arguments

Argument	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.
hash-length	Hash length is the 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.
priority	Priority assigned to this BSR. The software elects the BSR with the highest priority, or if the BSR priorities match, the software elects the BSR with the highest IP address. This value ranges from 0, the lowest priority, to 255 and has a default of 64.

You can configure a candidate RP with the arguments described in Table 3-5.

Table 3-5 BSR Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the BSR source IP address used in Bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP specified in a prefix format.
interval	Number of seconds between sending candidate-RP messages. This value ranges from 1 to 65,535 and has a default of 60 seconds. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
priority	Priority assigned to this RP. The software elects the RP with the highest priority for a range of groups, or if the priorities match, the highest IP address. This value ranges from 0, the highest priority, to 65,535 and has a default of 192.

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:

Step 1 Configure whether each router in the PIM domain should listen and forward BSR messages. A router configured as either a candidate RP or a candidate BSR will automatically listen to and forward all bootstrap router protocol messages, unless an interface is configured with the domain border feature. For more information, see the "Configuring PIM Sparse Mode" section on page 3-36.

Step 2 Select the routers to act as candidate BSRs and RPs.

Step 3 Configure each candidate BSR and candidate RP as described in this section.

Step 4 Configure BSR message filtering. See the "Configuring Message Filtering" section on page 3-52.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. **configure terminal**
2. **ip pim** [**bsr**] **bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*]
3. **ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* [**priority** *priority*] [**interval** *interval*]
4. (Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**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. For parameter details, see Table 3-4.
Step 3	**ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* [**priority** *priority*] [**interval** *interval*] **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. **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	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** switch(config)# show ip pim group-range	(Optional) Displays PIM modes and group ranges.
Step 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

Configuring Auto-RP

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

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 Table 3-6.

Table 3-6 Auto-RP Mapping Agent Arguments

Argument	Description
interface	Interface type and number used to derive the IP address of the Auto-RP mapping agent used in bootstrap messages.
scope *ttl*	Time-To-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32. **Note** See the border domain feature in the "Configuring PIM Sparse Mode" section on page 3-36.

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 described in Table 3-7.

Table 3-7 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. Specified in a prefix format.
scope *ttl*	Time-To-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32. **Note** See the border domain feature in the "Configuring PIM Sparse Mode" section on page 3-36.
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.

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:

Step 1 For each router in the PIM domain, configure whether that router should listen and forward Auto-RP messages. A router configured as either a candidate RP or an Auto-RP mapping agent will automatically listen to and forward all Auto-RP protocol messages, unless an interface is configured with the domain border feature. For more information, see the "Configuring PIM Sparse Mode" section on page 3-36.

Step 2 Select the routers to act as mapping agents and candidate RPs.

Step 3 Configure each mapping agent and candidate RP as described in this section.

Step 4 Configure Auto-RP message filtering. See the "Configuring Message Filtering" section on page 3-52.

BEFORE YOU BEGIN

Ensure that you have installed the LAN Base 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* [**scope** *ttl*] [**interval** *interval*]
4. (Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters 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. For parameter details, see Table 3-6.

	Command	Purpose
Step 3	**ip pim** {**send-rp-announce** | {**auto-rp rp-candidate**}} *interface* {**group-list** *ip-prefix* | **route-map** *policy-name}* [**scope** *ttl*] [**interval** *interval*] **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. For parameter details, see Table 3-7. **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	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM modes and group ranges.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring a PIM Anycast-RP Set

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

Step 1 Select the routers in the PIM Anycast-RP set.

Step 2 Select an IP address for the PIM Anycast-RP set.

Step 3 Configure each peer RP in the PIM Anycast-RP set as described in this section.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *number*
3. **ip address** *ip-prefix*
4. **exit**
5. **ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address*
6. Repeat Step 5 using the same *anycast-rp* for each peer RP in the RP set
7. (Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**interface loopback** *number* **Example:** `switch(config)# interface loopback 0`	Configures an interface loopback. This example configures interface loopback 0.
Step 3	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 192.0.2.3/32`	Configures an IP address for this interface. This example configures an IP address for the Anycast-RP.

Step 4	`exit`
	
	Example:
	`switch(config)# exit`
		Returns to configuration mode.

Step 5	**ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* **Example:** `switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31`	Configures a PIM Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 6	Repeat Step 5 using the same Anycast-RP address for each peer RP in the Anycast-RP set.	—
Step 7	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	(Optional) Displays PIM modes and group ranges.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Shared Trees Only for ASM

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

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.

BEFORE YOU BEGIN

Ensure that you have installed the LAN Base 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* | **all**]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**ip pim use-shared-tree-only group-list** *policy-name* **Example:** switch(config)# ip pim use-shared-tree-only group-list my_group_policy	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ip multicast** command. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.
Step 3	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** switch(config)# show ip pim group-range	(Optional) Displays PIM modes and group ranges.
Step 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

Configuring SSM

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

Note The Cisco NX-OS software does not support PIM SSM on vPCs. For more information about vPCs, see the *Cisco Nexus 5500 Series NX-OS Interfaces Configuration Guide, Release 6.0*.

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. For more information, see Chapter 2, "Configuring IGMP."

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

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

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**ip pim ssm range** {*ip-prefix* | **none**} | **route-map** *policy-name*} **Example:** switch(config)# ip pim ssm range 239.128.1.0/24	Configures up to four group ranges to be treated in SSM mode. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed.
	no ip pim ssm {**range** {*ip-prefix* | **none**} | **route-map** *policy-name*} **Example:** switch(config)# no ip pim ssm range none	Removes the specified prefix from the SSM range, or removes the route-map policy. If the keyword **none** is specified, resets the SSM range to the default of 232.0.0.0/8.

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

Configuring RPF Routes for Multicast

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

Multicast routes are used not to directly forward traffic but to make RPF checks. RPF routes for multicast cannot be redistributed. For more information about multicast forwarding, see the "Multicast Forwarding" section on page 1-4.

BEFORE YOU BEGIN

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

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** [**vrf** *vrf-name*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters 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 192.0.2.33/24 192.0.2.1	Configures an RPF route for multicast for use in RPF calculations. Route preference values range from 1 to 255. The default preference is 1.

	Command	Purpose
Step 3	**show ip static-route** [**vrf** *vrf-name*] **Example:** `switch(config)# show ip static-route`	(Optional) Displays configured static routes.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Route Maps to Control RP Information Distribution

You can configure route maps to help protect against some RP configuration errors and malicious attacks. You use route maps in commands that are described in the "Configuring Message Filtering" section on page 3-52.

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 ip multicast** command has an effect in the route map.

BEFORE YOU BEGIN

Ensure that you have installed the LAN Base Services license and enabled 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*]} | {**group** *ip-prefix* [**rp** *ip-address* [**rp-type** *rp-type*]]}
4. (Optional) **show route-map**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters 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. This configuration method uses the **permit** keyword.
Step 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {{**group-range** {gadrr_start to gadrr_end} | {**group** *ip-prefix}* {**source** source-ip-address}} **Example:** switch(config)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 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 examples.
Step 4	show route-map **Example:** switch(config-route-map)# show route-map	(Optional) Displays configured route maps.
Step 5	**copy running-config startup-config** **Example:** switch(config-route-map)# copy running-config startup-config	(Optional) Saves configuration changes.

Configuring Message Filtering

You can configure filtering of the PIM messages described in Table 3-8.

Table 3-8 PIM Message Filtering

Message Type	Description
Global to the switch	
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[1] where you can specify group or group and source addresses with the **match ip 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.

Table 3-8 PIM Message Filtering (continued)

Message Type	Description
BSR candidate RP policy	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy[1] where you can specify the RP and group addresses, and the type 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.
BSR policy	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy[1] 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.
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[1] where you can specify the RP and group addresses, and the type 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.
Auto-RP mapping agent policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy[1] 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.
Per switch interface	
Join-prune policy	Enables join-prune messages to be filtered based on a route-map policy[1] 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.

1. For information about configuring route-map policies, see the *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.0*.

For information about configuring multicast route maps, see the "Configuring Route Maps to Control RP Information Distribution" section on page 3-51.

BEFORE YOU BEGIN

Ensure that you have installed the LAN Base 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. **no switchport**
10. (Optional) **ip pim jp-policy** *policy-name* [**in** | **out**]
11. (Optional) **show run pim**
12. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**ip pim log-neighbor-changes** **Example:** switch(config)# ip pim log-neighbor-changes	(Optional) Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	**ip pim register-policy** *policy-name* **Example:** switch(config)# ip pim register-policy my_register_policy	(Optional) Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ip multicast** command.
Step 4	**ip pim bsr rp-candidate-policy** *policy-name* **Example:** switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy	(Optional) Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses, and the type ASM with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.
Step 5	**ip pim bsr bsr-policy** *policy-name* **Example:** switch(config)# ip pim bsr bsr-policy my_bsr_policy	(Optional) Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.
Step 6	**ip pim auto-rp rp-candidate-policy** *policy-name* **Example:** switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy	(Optional) Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses, and the type 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.

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

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

Step 9	**no switchport** **Example:** `switch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.
Step 10	**ip pim jp-policy** *policy-name [**in** | **out**]* **Example:** `switch(config-if)# ip pim jp-policy my_jp_policy`	(Optional) Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the **match ip multicast** command. The default is no filtering of join-prune messages. This command filters messages in both incoming and outgoing directions.

Step 11	`show run pim`
	
	Example:
	`switch(config-if)# show run pim`
		(Optional) Displays PIM configuration commands.

Step 12	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves configuration changes.

Binding VRFs to vPCs

You can bind a virtual routing and forwarding (VRF) instance to a virtual Port Channel (vPC) for the receivers in a non-vPC VLAN and the receivers connected to a Layer 3 interface to receive multicast traffic. The non-vPC VLANs represent the VLANs that are not trunked over a vPC peer-link.

You must create a VRF for vPC keepalive packets to prevent the vPC keep-alive link from being disrupted by the wrong routes learned through the dynamic routing protocol.

Note If you configure the **vpc bind-vrf** command to forward multicast traffic over the vPC peer link, you need to reload the switches to avoid any traffic loss.

BEFORE YOU BEGIN

Ensure that you have configured the vPC peers.

Ensure that you have configured a VRF.

SUMMARY STEPS

1. **configure terminal**
2. **vpc bind-vrf** *vrf-name* **vlan** *vlan-id*
3. (Optional) show vpc
4. (Optional) **show running-configuration pim**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	**vpc bind-vrf** *vrf-name* **vlan** *vlan-id* **Example:** switch(config)# vpc bind-vrf vrf-keepalive vlan 100	Binds a VRF instance to a vPC. **Note** You must use a reserved VLAN that is not already in use.
Step 3	**show vpc** **Example:** switch(config)# show vpc	(Optional) Shows the vPC configuration information.
Step 4	**show running-configuration pim** **Example:** switch(config)# show running-configuration pim	(Optional) Shows the running-configuration information for PIM, including the **feature** command.
Step 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

Restarting the PIM Processes

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

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

When you restart PIM, 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.

BEFORE YOU BEGIN

Ensure that you have installed the LAN Base 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

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

Step 2	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters 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	**show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	(Optional) Shows the PIM running-configuration information, including the **flush-routes** command.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Verifying the PIM Configuration

To display the PIM configuration information, perform one of the following tasks:

Command	Purpose
show ip mroute {*source group* | *group* [*source*]} [**vrf** *vrf-name* | **all**]	Displays the IP multicast routing table.
show ip pim df [**vrf** *vrf-name* | **all**]	Displays the designated forwarder (DF) information for each RP by interface.

Command	Purpose
show ip pim group-range [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see also the **show ip pim rp** command.
show ip pim interface [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays information by the interface.
show ip pim neighbor [**vrf** *vrf-name* | **all**]	Displays neighbors by the interface.
show ip pim oif-list *group* [*source*] [**vrf** *vrf-name* | **all**]	Displays all the interfaces in the OIF-list.
show ip pim route {source group | group [source]} [**vrf** *vrf-name* | **all**]	Displays information for each multicast route, including interfaces on which a PIM join for that (S, G) has been received.
show ip pim rp [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known to the software, how they were learned, and their group ranges. For similar information, see also the **show ip pim group-range** command.
show ip pim rp-hash [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information. For information about the RP hash, see RFC 5059.
show running-configuration pim	Displays the running-configuration information.
show startup-configuration pim	Displays the running-configuration information.
show ip pim vrf [*vrf-name* | **all**] [**detail**]	Displays per-VRF information.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*.

Displaying Statistics

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

This section has the following topics:

- Displaying PIM Statistics, page 58
- Clearing PIM Statistics, page 59

Displaying PIM Statistics

You can display the PIM statistics and memory usage using the commands listed in Table 3-9. Use the **show ip** form of the command for PIM.

Table 3-9 PIM Statistics Commands

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

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*.

Clearing PIM Statistics

You can clear the PIM statistics using the commands listed in Table 3-10. Use the **show ip** form of the command for PIM.

Table 3-10 PIM Commands to Clear Statistics

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

Configuration Examples for PIM

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

This section includes the following topics:

- Configuration Example for SSM, page 59
- Configuration Example for BSR, page 60
- Configuration Example for PIM Anycast-RP, page 61

Configuration Example for SSM

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

Step 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)# no switchport
switch(config-if)# ip pim sparse-mode
```

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

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp version 3
```

Step 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
```

Step 4 Configure message filtering.

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

This example shows how to configure PIM SSM mode:

```
configure terminal
  interface ethernet 2/1
    no switchport
    ip pim sparse-mode
    ip igmp version 3
    exit
  ip pim ssm range 239.128.1.0/24
  ip pim log-neighbor-changes
```

Configuration Example for BSR

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

Step 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)# no switchport
switch(config-if)# ip pim sparse-mode
```

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

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

Step 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
```

Step 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
```

Step 5 Configure message filtering.

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

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

```
configure terminal
  interface ethernet 2/1
    no switchport
    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
```

Configuration Example for PIM Anycast-RP

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

Step 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)# no switchport
switch(config-if)# ip pim sparse-mode
```

Step 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
```

Step 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
```

Step 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
```

Step 5 Configure message filtering.

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

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

```
configure terminal
```

```
interface ethernet 2/1
  no switchport
  ip pim sparse-mode
  exit
interface loopback 0
  ip address 192.0.2.3/32
  exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
ip pim log-neighbor-changes
```

Where to Go Next

You can configure the following features that work with PIM:

- Chapter 2, "Configuring IGMP"
- Chapter 4, "Configuring IGMP Snooping"
- Chapter 5, "Configuring MSDP"

Additional References

For additional information related to implementing PIM, see the following sections:

- Related Documents, page 62
- Standards, page 62
- Appendix A, "IETF RFCs for IP Multicast"

Related Documents

Related Topic	Document Title
CLI commands	*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*
Configuring VRFs	*Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.0*

Standards

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