Configuring PIM

This chapter describes how to configure the Protocol Independent Multicast (PIM) features on Cisco Nexus 3600 platform switches in your IPv4 networks.

This chapter includes the following sections:

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.

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.

Note Cisco Nexus 3600 platform switches do 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 Configuring IGMP.

Note Cisco Nexus 3600 platform switches do not support PIM6.

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.
- Source-Specific Multicast (SSM) builds a source tree that originates 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.

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

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

Note Multicast equal-cost multipathing (ECMP) is on by default in the Cisco NX-OS for the Cisco Nexus 3548 Switch; 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.

PIM SSM with vPC

You can enable PIM SSM on Cisco Nexus 3600 platform switches with an upstream Layer 3 cloud along with the vPC feature. If there are no downstream PIM neighbors, you can form a PIM neighbor relationship between two switches over a vPC VLAN through a vPC peer link.

Hello Messages

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

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. The IGMP snooping software also processes PIM hello messages.

For information about configuring hello message authentication, see the Configuring PIM Sparse Mode section.

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 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.

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.

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 within 180 seconds, 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 switch

For information about configuring static RPs, see the Configuring Static RPs section.

BSRs

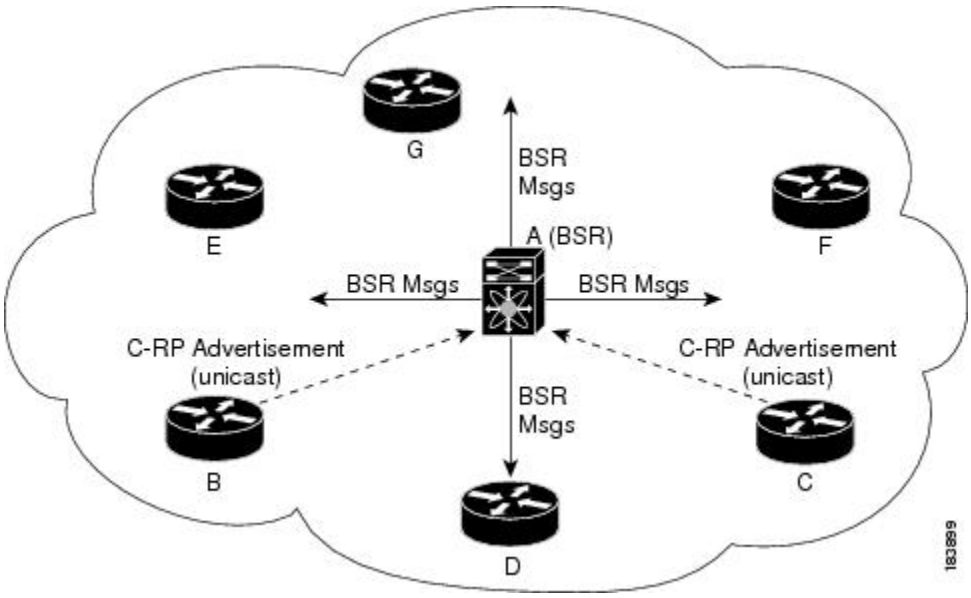
The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs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

The following figure 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 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.

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 and Configuring Static RPs section.

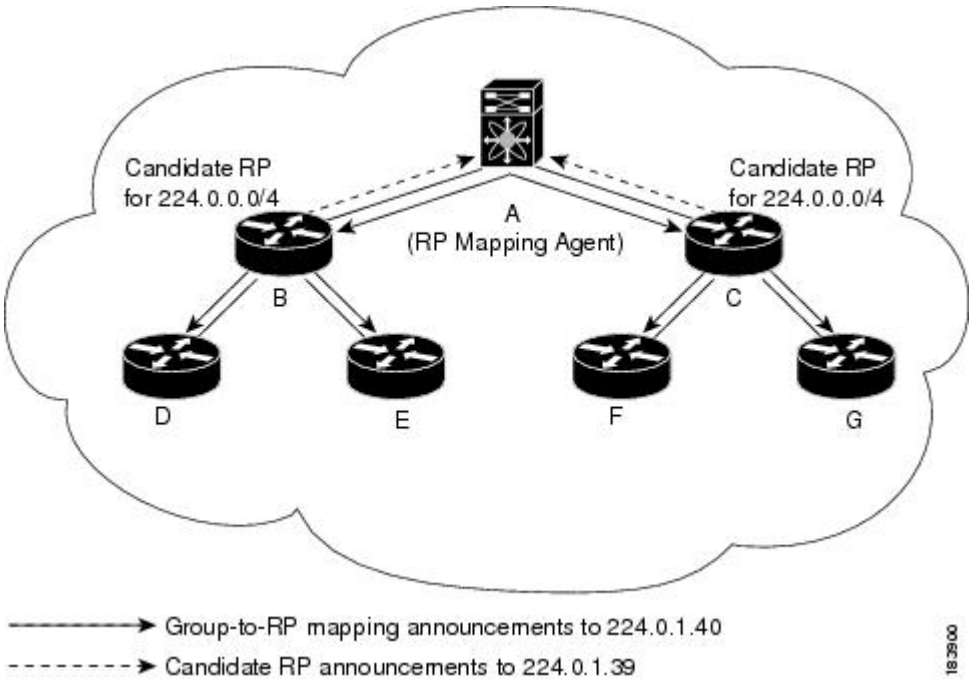
Auto-RP

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.

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

The following 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.

For information about configuring Auto-RP, see the Configuring Auto RP section.

Anycast-RP

Anycast-RP has two implementations: one uses Multicast Source Discovery Protocol (MSDP) and the other is based on RFC 4610. 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 (PIM) section.

PIM Register Messages

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

- To notify the RP that a source is actively sending to a multicast group.

- To deliver multicast packets sent by the source to the RP for delivery down the shared tree.

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

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

You can use the **ip pim register-source** command to configure the IP source address of register messages when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation might occur if the source address is filtered so that the packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address fails 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:

```
switch # configuration terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim register-source ethernet 2/3
switch(config-vrf)#
```

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 Message Filtering section.

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 PIM SSM with vPC section.

In SSM mode, the DR triggers (S, G) PIM join 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.

In ASM mode, the DR triggers (S, G) or (*, G) PIM join messages toward the source depending on the IGMP membership reports that it receives. When a DR receives an IGMP membership report from a directly connected host or receiver, the shortest path is formed to the RP. Additionally, the DR is responsible for sending PIM register messages to the RP when the source becomes active. The result is a shared tree that connects all sources transmitting to the same multicast group with all the receivers of that group.

For information about configuring the DR priority, see the Configuring PIM Sparse Mode section.

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 Message Filtering section.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value. For more information, see the Configuring Auto RP section.

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 3600 NX-OS Unicast Routing Configuration Guide.

Prerequisites for PIM

PIM has the following prerequisites:

- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

Guidelines and Limitations for PIM

PIM has the following guidelines and limitations:

- Cisco Nexus 3600 platform switches do not support PIM adjacency with a vPC leg or with a router behind a vPC.
- The loopback interface that is used as an RP in multicast must have the ip pim sparse-mode configuration. This is an extra configuration guideline.
- PIM does not interoperate with any version of PIM dense mode or PIM Sparse Mode version 1.
- PIM6 is not supported.
- PIM Bidir is not supported.
- We recommend that you do not configure both Auto-RP and BSR protocols in the same network.
- Configure candidate RP intervals to a minimum of 15 seconds.
- You must configure PIM on the loopback interface that is used for the PIM Anycast-RP.
- Only VRF-lite (no import or export) is supported with PIM.

Default Settings for PIM

The following table lists the default settings for PIM parameters.

Table 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
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 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 below.

Table 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, **PIM Multicast Distribution Modes**, select the range of multicast groups that you want to configure in each mode.

Step 2 Enable the PIM or PIM6 features. See the Enabling the PIM Feature section.

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.

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.
- For SSM mode, see the Configuring SSM (PIM) section.
- For RPF routes for multicast, see the Configuring RPF Routes for Multicast section.

Step 5 If you are configuring message filtering. See the Configuring Message Filtering section.

Enabling the PIM Feature

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.

Procedure

	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.

	Command or Action	Purpose
Step 3	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Shows the running-configuration information for PIM, including the **feature** command.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

Note For information about configuring multicast route maps, see the Configuring Route Maps to Control RP Information Distribution section.

Note To configure the join-prune policy, see the Configuring Message Filtering section.

Before you begin

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

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
Step 4	(Optional) **ip pim rp** [*ip prefix*] **vrf** *vrf-name*| **all** **Example:** `switch(config)# show ip pim rp`	Displays PIM RP information, including Auto-RP and BSR listen and forward states.
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) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays PIM running-configuration information, including the register rate limit.

Step 7	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as **ethernet** *slot/port.*

Step 8	**no switchport** **Example:** `sswitch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.
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	(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 11	(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
Step 12	(Optional) **ip pim hello-authentication keychain** *name* **Example:**	Enables the keychain authentication on a PIM interface. Where <keychain> is the name of a keychain.

	Command or Action	Purpose
	`switch(config-if)# ip pim hello-authentication keychain mykeychain`	**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 13	(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 1 to 4294967295. The default is 30000. **Note** The minimum value is 1 millisecond.
Step 14	(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 15	(Optional) **ip pim neighbor-policy** *policy name* **Example:** `switch(config-if)# ip pim neighbor-policy my_neighbor_policy`	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	(Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	Displays PIM interface information.
Step 17	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	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.

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.

Note We recommend that the RP address uses the loopback interface.

Before you begin

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

Procedure

	Command or Action	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	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] **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`	Saves configuration changes.

Configuring BSRs

You configure BSRs by selecting candidate BSRs and RPs.

Note We recommend that you 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 following table.

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	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 and keywords described in Table 4.

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 minim of 15 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 highest value between 0 and 255.

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 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.
2. Select the routers to act as candidate BSRs and RPs.
3. Configure each candidate BSR and candidate RP as described in this section.
4. Configure BSR message filtering. See the Configuring Message Filtering section.

Configuring BSRs

Before you begin

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

Procedure

	Command or Action	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 10.
Step 3	**ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **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	(Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
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 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 the following table.

Table 5: Auto-RP Mapping Agent Arguments

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

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 the following 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. 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 Mod section.
interval	Number of seconds between sending RP-Announce messages. This valu 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:

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.
2. Select the routers to act as mapping agents and candidate RPs.
3. Configure each mapping agent and candidate RP as described in this section.
4. Configure Auto-RP message filtering. See the Configuring Message Filtering section.

Configuring Auto RP

Before you begin

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

Procedure

	Command or Action	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 **Auto-RP Mapping Agent Arguments**.
Step 3	**ip pim** {**send-rp-announce** | {**auto-rp rp-candidate**}} interface **group-list** *ip-prefix* [**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. For parameter details, see table **Auto-RP Candidate RP Arguments and Keywords**. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures ASM candidate RP.
Step 4	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] **Example:**	Displays PIM modes and group ranges.

	Command or Action	Purpose
	`switch(config)# show ip pim group-range`	
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring a PIM Anycast RP Set (PIM)

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 and local address in the PIM Anycast-RP set as described in this section.

Before you begin

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

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	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 192.168.1.1/32`	Configures an IP address for this interface. This example configures an IP address for the Anycast-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	**exit** **Example:** `switch(config)# exit`	Returns to configuration mode.
Step 6	**ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* **Example:**	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

	Command or Action	Purpose
	`switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31` `switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.32`	addresses of RPs are used for communication with RPs in the set. The example shows an Anycast-RP set of 192.0.2.31 and 192.0.2.32, and the Anycast-RP used in the network would be 192.0.2.3.
Step 7	Repeat Step 6 using the same Anycast-RP address for each peer RP in the Anycast-RP set.	—
Step 8	**show ip pim group-range** [*ip-prefix*] [**vrf** { *vrf-name* | **all** }]	Displays PIM modes and group ranges.
Step 9	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring Shared Trees Only for ASM

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

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 Enterprise Services license and enabled PIM.

Procedure

	Command or Action	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.

	Command or Action	Purpose
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] **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`	Saves configuration changes.

Setting the Maximum Number of Entries in the Multicast Routing Table

You can set the maximum number of entries in the multicast routing table (MRT).

Before you begin

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

Procedure

	Command or Action	Purpose

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

Step 2	**hardware profile multicast max-limit** *max-entries* **Example:** `switch(config)# hardware profile multicast max-limit 3000`	Sets the maximum number of entries in the multicast routing table. The maximum number of entries in the multicast routing table can range from 0 to 8000.
Step 3	(Optional) **show hardware profile status** **Example:** `switch(config)# show hardware profile status`	Displays information about the multicast routing table limits.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring SSM (PIM)

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

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

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.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

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.

(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.

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. You can override the default range by using this command. The command in the example overrides the default range to 234.0.0.0/24.

	Command or Action	Purpose
		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
Step 4	(Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** { *vrf-name* | **all** }] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

Before you begin

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

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* |} [*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 preferenceis 1.
Step 3	(Optional) **show ip static-route** [**vrf** *vrf-name*] **Example:** `switch(config)# show ip static-route`	Displays configured static routes.
Step 4	(Optional) **copy running-config startup-config**	Saves configuration changes.

Disabling Multicast Multipath

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

Procedure

	Command or Action	Purpose

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

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

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 this section.

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.

Before you begin

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

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

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** *ip-prefix*]} | {**group** *ip-prefix* **rp** *ip-address* [**rp-type** *rp-type*]} **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 or Bidir). This configuration method requires the group and RP specified as shown in the examples.
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`	Saves configuration changes.

Configuring Message Filtering

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

Table 7: PIM and PIM6 Message Filtering

Message Type	Description
Global to the switch	
PIM register policy	Enables PIM register messages to be filtered based on a route-map policy,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.
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 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, 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.

Message Type	Description
Auto-RP candidate RP policy	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map 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.
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.
Per Switch 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.

For information about configuring multicast route maps, see the Configuring Route Maps to Control RP Information Distribution section.

Configuring Message Filtering

Before you begin

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

Procedure

	Command or Action	Purpose

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

Step 2	(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 3	(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 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.

	Command or Action	Purpose
Step 4	(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 5	(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 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 6	(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 7	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 8	**no switchport** **Example:** `switch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.
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. This command filters messages in both incoming and outgoing directions.
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`	Saves configuration changes.

Flushing the Routes

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.

Procedure

	Command or Action	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`	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`	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* [*source*]} [**vrf** *vrf-name* | **all**]	Displays the IP multicast routing table.
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.
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 3000 Series Command Reference.

Displaying Statistics

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

Displaying PIM Statistics

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

Table 8: PIM Statistics Commands

Command	Description
show ip pim policy statistics	Displays policy statistics for Register, RP, and join-prune message policies.

Clearing PIM Statistics

You can clear the PIM statistics using the commands listed in the following Table.

Table 9: PIM Commands to Clear Statistics

Command	Description
clear ippim 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.

Configuration Example for SSM

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

1. **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
   ```

2. **Step 2**: Configure the parameters for IGMP that support SSM. See 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
   ```

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
   ```

4. **Step 4**: Configure message filtering.

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

This example shows how to configure PIM in 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 PIM SSM Over vPC

This example shows how to override the default SSM range of 232.0.0.0/8 to 225.1.1.1/32. No special configuration is required to support PIM SSM over vPC. If you choose to change the default SSM to a different range (for example, to 225.1.1.1), this example shows you how to do it.

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim ssm range 225.1.1.1/32
switch(config-vrf)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range Action Mode RP-address Shrd-tree-range Origin
225.1.1.1/32 Accept SSM - - Local

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: 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

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 Eth9/5
101 225.1.1.1 v3
100.6.160.20 D Eth9/3

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 Eth9/5
101 225.1.1.1 v3
100.6.160.20 D Eth9/3


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

PIM SSM Over vPC Configuration Example
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)
```

Configuration Example for BSR

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

1. **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
   ```

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

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

3. **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
```

4. **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
```

5. **Step 5**: Configure message filtering.

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

6. **Step 6**: Verify the BSR operation.

```
switch# show ip pim rp
```

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:

1. **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
```

2. **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
```

3. **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
```

4. **Step 4**: Because the router is also an Anycast-RP peer, configure a unique peer address (which is routable domain wide) on an interface (for example, loopback 2).

```
switch# configure terminal
switch(config)# interface loopback 2
switch(config-if)# ip address 193.0.2.31/32
switch(config-if)# ip pim sparse-mode
```

Note A similar configuration needs to be done on all Anycast peer routers with their uniquely routable addresses.

5. **Step 5**: Add all of the Anycast peers into an RP set.

```
switch# configure terminal
switch(config)# interface loopback 2
switch(config-if)# ip pim anycast-rp 192.0.2.3 193.0.2.31
switch(config-if)# ip pim anycast-rp 192.0.2.3 193.0.2.32
```

Note You can use a similar configuration to create multiple RP sets.

6. **Step 6**: Verify the Anycast-RP operation.

```
switch# show ip pim interface brief
switch# show ip pim rp
```

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
```

Where to Go Next

You can configure the following features that work with PIM:

- Configuring IGMP
- Configuring IGMP Snooping

Additional References

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

- Related Documents

- MIBs

Related Documents

Related Topic	Document Title
Configuring VRFs	Cisco Nexus 3600 NX-OS Unicast Routing Configuration Guide

MIBs

MIBs	MIBs Link
IPMCAST-MIB	To locate and download MIBs, go to the following URL: http://mibs.cloudapps.cisco.com/ITDIT/MIBS/MainServlet