PIM Allow RP

This module describes how to configure the PIM Allow RP feature in IPv4 or IPv6 networks for inter-connecting Protocol Independent Multicast (PIM) Sparse Mode (SM) domains with different rendezvous points (RPs). PIM Allow RP enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This allows the receiving device to accept the (*, G) Join from the different RP.

- Finding Feature Information, page 1
- Restrictions for PIM Allow RP, page 1
- Information About PIM Allow RP, page 2
- How to Configure PIM Allow RP, page 3
- Configuration Examples for PIM Allow RP, page 8
- Additional References for PIM Allow RP, page 10
- Feature Information for PIM Allow RP, page 11

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for PIM Allow RP

- PIM Allow RP only supports connecting PIM SM domains.
- PIM Allow RP is applicable for downstream traffic only, that is, it is only applicable for building the shared tree.

- PIM Allow RP does not work with Auto-RP or Boot Strap Router (BSR). Only static configuration is supported. However, it does allow the embedded RP in the consumer network to be different than the one configured statically in the service provider network.

Information About PIM Allow RP

Rendezvous Points

A rendezvous point (RP) is a role that a device performs when operating in Protocol Independent Multicast (PIM) Sparse Mode (SM). An RP is required only in networks running PIM SM. In the PIM-SM model, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic.

This method of delivering multicast data is in contrast to PIM Dense Mode (PIM DM). In PIM DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop device of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

In most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

PIM Allow RP

There are three types of networks: publisher, consumer, and transport. Many publisher networks can originate content and many consumer networks can be interested in the content. The transport network, owned and operated by a service provider, connects the publisher and the consumer networks.

The consumer and the transport networks are connected as follows:

For a specific group range, or all-groups range (similar to a default route), the service provider defines a particular rendezvous point (RP), such as RP-A. Reverse path forwarding of RP-A from a consumer device will cause a (*,G) Join to be sent towards the transport network.

For the same group, the service provider may define a different RP, such as RP-B, that is used to build the shared tree within the transport network for G. RP-A and RP-B are typically different RPs and each RP is defined for different group ranges.

RFC 4601 dictates that if a device receives a (*, G) Join and the RP that is specified in the (*, G) Join is different than what the receiving device expects (unknown RPs), the incoming (*, G) Join must be ignored. The PIM Allow RP feature enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This allows the receiving device to accept the (*, G) Join from the different RP.

PIM Allow RP is only applicable for downstream traffic, for building the shared tree. It does not work with Auto-RP or BSR. Only static configuration is supported. However, PIM Allow RP does compensate for the

embedded RP in the consumer network to be different than the one configured statically in the transport network.

How to Configure PIM Allow RP

Configuring RPs for PIM-SM

Before You Begin

All access lists should be configured prior to beginning the configuration task. For information about how to configure an access list, see the "Creating an IP Access List and Applying It to an Interface" module of the *Security Configuration Guide: Access Control Lists* guide.

For IPv6 network devices, you must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. • **ip multicast-routing** [**vrf** *vrf-name*] **distributed**
   • **ipv6 multicast-routing** [**vrf** *vrf-name*]
4. **interface** *type number*
5. • **ip pim sparse-mode**
   • **ipv6 pim enable**
6. **ipv6 address** {*ipv6-address* | *prefix-length* | *prefix-name sub-bits* | *prefix-length*}
7. **no shut**
8. **exit**
9. Repeat Steps 4 through 8 on every interface that uses IP multicast.
10. • **ip pim** [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**]
    • **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*]
11. **exit**
12. **show ip pim rp** [**mapping**] [*rp-address*]
13. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	• **ip multicast-routing** [**vrf** *vrf-name*] **distributed**
	• **ipv6 multicast-routing** [**vrf** *vrf-name*]
	
	Example:
	`Device(config)# ip multicast-routing`
	`Device(config)# ipv6 multicast-routing`
		• For IPv4: Enables multicast routing on all interfaces of the device. In Cisco IOS XE Release 3.2S and earlier releases, the **distributed** keyword is optional.
		• For IPv6: Enables multicast routing on all interfaces of the device and also enables multicast forwarding for PIM and MLD on all multicast-enabled interfaces of the device.
		Note IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. On certain devices, the IPv6 multicast routing must also be enabled in order to use IPv6 unicast routing.

Step 4	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.

Step 5	• **ip pim sparse-mode**
	• **ipv6 pim enable**
	
	Example:
	`Device(config-if)# ip pim sparse-mode`
	`Device(config-if)# ipv6 pim enable`
		• For IPv4: Enables PIM. You must use sparse mode.
		• For IPv6: Enables IPv6 and by default, IPv6 PIM.

Step 6	**ipv6 address** {*ipv6-address* | *prefix-length* | *prefix-name sub-bits* | *prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8::4:4/64`	For IPv6 only: Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 7	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Device(config-if)# exit`	— Returns to global configuration mode.
Step 9	Repeat Steps 4 through 8 on every interface that uses IP multicast.	

Step 10	• **ip pim** [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**]
	• **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*]
	
	Example:
	`Device(config)# ip pim rp-address 192.0.2.1 acl-sparse`
	
	`Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`
		• For IPv4: Configures the address of a PIM RP. If no access list is specified, the RP address is applied to all multicast groups, 224/4.
		• For IPv6: Configures the address of a PIM RP. If no group-address list is specified, the RP address is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96.

Step 11	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 12	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Device# show ip pim rp mapping`	(Optional) Displays RPs known in the network and shows how the router learned about each RP.
Step 13	**show ip mroute** **Example:** `Device# show ip mroute`	(Optional) Displays the contents of the IP mroute table.

Enabling PIM Allow RP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. • **ip pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
   • **ipv6 pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	• **ip pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
	• **ipv6 pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
	
	Example:
	`Device(config)# ip pim allow-rp`
	`Device(config)# ipv6 pim allow-rp`
		Enables PIM Allow RP.

Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Displaying Information About PIM-SM and RPs

SUMMARY STEPS

1. **enable**
2. • **show ip pim** [**vrf** *vrf-name*] **rp** [**metric**] [*rp-address*]
   • **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
3. • **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]
   • **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	• **show ip pim** [**vrf** *vrf-name*] **rp** [**metric**] [*rp-address*]
	• **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
	
	Example:
	`Device# show ip pim interface`
	`Device# show ipv6 pim interface`
		Displays information about interfaces configured for PIM.

Step 3	• **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]
	• **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]
	
	Example:
	`Device# show ipv6 pim rp mapping`
	`Device# show ipv6 pim group-map static`
		Displays the mappings for the PIM group to the active rendezvous points.

Configuration Examples for PIM Allow RP

Example: IPv4 PIM Allow RP

In the following example:

1. The downstream device loopback (Loopback100) creates a static (*,239.1.2.3) Join to a nonexistent RP (11.30.3.3).
2. The static route makes the device think that this RP can be reached through the upstream device via 11.10.2.1, causing the downstream device to send a (*,239.1.2.3) PIM Join with an RP address (11.30.3.3) to the upstream router.
3. When the upstream device receives the (*,239.1.2.3) PIM Join, it realizes that the RP address in the Join (11.30.3.3) is different from the known (configured) interface-to-RP address (11.10.3.3).
4. The PIM allow RP configuration on the upstream device permits the (*,239.1.2.3) to be processed and creates a (*,239.1.2.3) join to the RP (11.10.3.3).

Note If the **pim allow-rp** command is not configured on the upstream device, the upstream device must ignore Joins with different RPs.

```
###################
#   Downstream
###################
!
hostname downstream-router
!
!
ip multicast-routing distributed
!
!
interface Loopback100
ip address 101.10.1.2 255.255.255.0
ip igmp static-group 239.1.2.3
ip pim sparse-dense-mode
no shut
!
interface Ethernet1/2
ip address 11.10.2.2 255.255.255.0
ip pim sparse-dense-mode
no shut
!
router ospf 200
network 11.0.0.0 0.255.255.255 area 1
network 101.0.0.0 0.255.255.255 area 1
!
ip pim rp-address 11.30.3.3
ip mroute 11.30.3.3 255.255.255.255 11.10.2.1
!
end


###################
#   Upstream
###################
!
hostname Upstream-router
!
!
```

```
ip multicast-routing distributed
!
!
interface FastEthernet0/0/2
ip address 11.10.2.1 255.255.255.0
ip pim sparse-dense-mode
no shut
!
interface FastEthernet0/0/4
! interface to RP (11.10.3.3)
ip address 10.10.4.1 255.255.255.0
ip pim sparse-dense-mode
no shut
!
router ospf 200
network 10.0.0.0 0.255.255.255 area 1
network 11.0.0.0 0.255.255.255 area 1
!
ip pim rp-address 11.10.3.3
ip pim allow-rp
!
end
```

Example: IPv6 PIM Allow RP

In the following example:

1. The downstream device loopback creates an static (*,FF03::1) Join to a non-existent RP (80::1:1:3).
2. The static route makes the device think that this RP can be reach via the upstream device via 10::1:1:1 and causes the downstream device to send a (*,FF03::1) PIM Join with an RP address (80::1:1:3) to the upstream device.
3. When the upstream device receives the (*,FF03::1) PIM Join, it realizes that the RP address in the Join (80::1:1:3) is different from the (known) configured address (20::1:1:3).
4. The PIM allow RP configuration on the upstream device permits the (*,FF03::1) to be processed, and creates a (*,FF03::1) Join to the RP (20::1:1:3).

Note If the **pim allow-rp** command is not configured on the upstream device, the upstream device must ignore Joins with different RPs .

```
##################
# Downstream
##################

!
hostname downstream-router
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface Loopback100
ipv6 address FE80::50:1:2 link-local
ipv6 address 50::1:1:2/64
ipv6 enable
ipv6 ospf 1 area 0
ipv6 mld join-group FF03::1
!
```

```
interface Ethernet1/2
ipv6 address FE80::10:1:2 link-local
ipv6 address 10::1:1:2/64
ipv6 enable
ipv6 ospf 1 area 0
no keepalive
!
!
ipv6 pim rp-address 80::1:1:3
ipv6 route 80::1:1:3/128 10::1:1:1 multicast
!
ipv6 router ospf 1
router-id 205.2.0.2
!
!
end


####################
#  Upstream
####################
!
hostname Upstream-router
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface FastEthernet0/0/2
ipv6 address FE80::10:1:1 link-local
ipv6 address 10::1:1:1/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface FastEthernet0/0/3
! interface to the RP (20::1:1:3)
ipv6 address FE80::20:1:1 link-local
ipv6 address 20::1:1:1/64
ipv6 enable
ipv6 ospf 1 area 0
!
!
ipv6 pim rp-address 20::1:1:3
ipv6 pim allow-rp
!
ipv6 router ospf 1
router-id 205.1.0.1
!
!
end
```

Additional References for PIM Allow RP

Standards and RFCs

Standard/RFC	Title
RFC 4601	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PIM Allow RP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for PIM Allow RP

Feature Name	Releases	Feature Information
PIM Allow RP	15.2(4)T Cisco IOS XE Release 3.7S 15.3(1)T	The PIM Allow RP feature enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This process permits the receiving device to accept the (*, G) Join from a different RP. The following commands were introduced or modified: **ip pim allow-rp**, **ipv6 pim allow-rp**.