Configuring PIM Allow RP

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

Introduction

This chapter describes how to configure the PIM Allow RP feature in IPv4 and 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.

Guidelines and Limitations 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 is restricted to use only the route-map.
- PIM Allow RP does not support the IPv6 Multicast prior to Cisco NX-OS Release 10.2(2)F.
- IPv6 PIM Allow RP is supported from Cisco NX-OS Release 10.2(2)F.
- PIM Allow RP does not support the RPM with “Source”. PIM Allow RP Information AboutPIM AllowRP.
- When the Allow-RP configuration is added with a non-existent RPM, all Joins/Prunes get rejected.
- When the Allow-RP configuration is added with an RPM having PERMIT-ALL or DENY-ALL, all Joins/Prunes are either accepted or discarded accordingly.

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 contrasts with 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 is introduced in Cisco NX-OS Release 8.4(1). This 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. A route-map is used to control which RP address and/or group addresses the (*,G) join is for. The RP address and the group address in the (*,G) join message is matched against any RP and group addresses specified in the route-map.

PIM Allow RP is only applicable for downstream traffic.

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 "Configuring IP ACLs" chapter in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Procedure

	Command or Action	Purpose

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

Step 2	**interface***interface*
	Example:
	`switch(config)# interface gigabitethernet 1/0/0`
	`switch(config-if)#`
		Selects an interface that is connected to hosts on which PIM can be enabled. **interface** type number.

Step 3	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enable PIM. You must use sparse mode.
Step 4	**no shut** **Example:** `switch(config-if)# no shut`	Enable an interface.
Step 5	**Exit** **Example:** `switch(config-if)# exit`	Return to global configuration mode. Repeat Steps 3 through 5 on every interface that uses IP multicast.
Step 6	**ip pim rp-address** *rp-address*[**group-list***ip-prefix* | **route-map***policy-name*] **Example:** `switch(config)# ip pim rp-address 30.2.2.2 group-list 224.0.0.0/4`	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. This command can also be used in VRF mode.
Step 7	**end** **Example:** `Switch (config)# end`	Exit the route map configuration mode.
Step 8	(Optional) **show ip pim rp** [**vrf**|*rp-address*] **Example:**	Display the RPs known in the network and shows how the router learned about each RP.

	Command or Action	Purpose
	`switch# show ip pim rp`	
Step 9	(Optional) **show ip mroute** **Example:** `switch# show ip mroute`	Display the contents of the IP mroute table.

Enabling PIM Allow RP

In the following configuration steps, you can configure one of the combinations of RPM at a time —group only, RP only, group RP, group-range only.

Procedure

	Command or Action	Purpose

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

Step 2	**route-map** *map-name* [**permit**|**deny**][*sequence-number* **Example:** `switch(config)# route-map mcast-grp permit 10`	Enter route-map configuration mode. Note that this configuration method uses the permit keyword.
Step 3	**match ip multicast group***group-address* **Example:** `Switch(config-route-map)# match ip multicast group 224.0.0.0/4`	Match the IP multicast group. **Note** You can configure only one combination of RPM at a time - group only, RP only, group RP, group-range only. For example, if you configure this step (group only), you must go to step 9. This is applicable to the below mentioned steps as well (from step-4 to step-8).
Step 4	**match ip multicast group-range** {*group address_start to group address_end*} **Example:** `switch(config-route-map) # match ip multicast group-range 230.1.1.1 to 230.1.1.255`	Match the IP multicast group range from/to the specified group address.
Step 5	**match ip multicast rp***rp-address* **Example:** `switch (config-route-map) # match ip multicast 222.0.0.0/4`	Match the IP multicast and the RP specified.

	Command or Action	Purpose
Step 6	**match ip multicast rp** *rp-address***rp-type***type* **Example:** `switch (config-route-map)# match ip multicast rp 1.1.1.1/32 rp-type ASM`	Match the IP multicast RP address and the RP type specified. ASM is the only supported RP type.
Step 7	**match ip multicast group** *address***rp***address* **Example:** `switch(config-route-map)# match ip multicast group 230.1.1.1/4 rp 1.1.1.1/32`	Match the IP multicast group address and the RP address.
Step 8	**match ip multicast group-range** {*group address_start to group address_end*}**rp***address* **Example:** `switch (config-route-map)# match ip multicast group-range 230.1.1.1 to 230.1.1.255 rp 1.1.1.1/32`	Matches the IP multicast group range from/to the specified address and the RP address.
Step 9	**ip pim allow-rp** *route-map-name* **Example:** `switch(config-roiute-map)# ip pim allow-rp test-route-map`	Enable PIM Allow RP; and allow sparse-mode RP addresses. This command is configured at the VRF level also. A route-map is used to control which RP address and/or group addresses the (*,G) join is for. The RP address and the group address in the (*,G) join message is matched against any RP and group addresses specified in the route-map.
Step 10	**ipv6 pim allow-rp** *route-map-name* **Example:** `switch(config-roiute-map)# ipv6 pim allow-rp test-route-map`	Enable the IPv6 PIM Allow RP.
Step 11	(Optional) **show ip pim policy statistics allow-rp-policy** **show ipv6 pim policy statistics allow-rp-policy** **Example:** `switch(config)# show ip pim policy statistics allow-rp-policy`	To view the policy statistics.
Step 12	**end** **Example:** `Switch (config-route-map)# end`	Exit the route map configuration mode.

Displaying Information About Allow RP Policy

The following commands can be used under VRF mode also.

Procedure

	Command or Action	Purpose
Step 1	**Enable** **Example:** `switch# enable`	Enable privileged EXEC mode.
Step 2	**show ip pim policy statistics allow-rp-policy** **Example:** `switch# show ip pim policy statistics allow-rp-policy`	Display the statistics about the current allow RP policy and its counters.
Step 3	**show ipv6 pim policy statistics allow-rp-policy** **Example:** `switch# show ipv6 pim policy statistics allow-rp-policy`	Display the IPv6 statistics about the current allow RP policy.
Step 4	**clear ip pim policy statistics allow-rp-policy** **Example:** `switch# clear ip pim policy statistics allow-rp-policy`	Clears the policy and counters of the allow RP policy.
Step 5	**clear ipv6 pim policy statistics allow-rp-policy** **Example:** `switch# clear ipv6 pim policy statistics allow-rp-policy`	Clears the policy and counters of the allow RP policy for IPv6.