Policy-Based Routing (PBR)

Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps9536/prod_command_reference_list.html

  http://www.cisco.com/en/US/products/ps11845/prod_command_reference_list.html

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.0SY supports only Ethernet interfaces. Cisco IOS Release 15.0SY does not support any WAN features or commands.

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Prerequisites for PBR

None.

Restrictions for PBR

The PFC and any DFCs provide the hardware support for the following:

- These IPv4 PBR commands:
  - **match ip address**
  - **match length**
  - **set ip next-hop** (2,000 instances)
  - **set ip default next-hop**
  - **set interface null0**
  - **set default interface null0**
  - **set ip vrf**
  - **set ip default vrf**
- If the RP address falls within the range of a PBR ACL, traffic addressed to the RP is policy routed in hardware instead of being forwarded to the RP. To prevent policy routing of traffic addressed to the RP, configure PBR ACLs to deny traffic addressed to the RP.
- Local PBR.
- IPv4 PBR recursive next-hop with load balancing.
- IPv6 PBR is supported in software.
- IPv6 PBR recursive next-hop is not supported.

Note IPv4 PBR recursive next-hop with reload balancing is not supported on Supervisor Engine 720.

Note Local PBR does not support routing of distributed Netflow Data Export.

Information About PBR

PBR Overview

PBR is an alternative to routing protocols and allows you to configure a policy for unicast traffic flows, which provides more control over routing than a routing protocol does and avoids the need to configure interface-level traffic classification. PBR can route unicast traffic along a different path than a routing protocol would use. PBR can provide:

- Equal access
- Protocol-sensitive routing
- Source-sensitive routing
- Routing based on interactive rather than batch traffic

- Routing based on dedicated links

PBR route maps can be configured to do the following:

- Allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets or a combination of these values.
- Classify traffic based on extended access list criteria.
- Set IP precedence bits.
- Route packets to specific paths.

PBR applies a route map to all ingress unicast traffic received on a PBR-enabled interface. PBR cannot be applied to egress traffic or to multicast traffic.

If the ingress unicast traffic does not match any route map statements, the route map applies all the configured set clauses. Routing protocols forward traffic that matches a route-map deny statement and traffic that does not match any route-map permit statements.

PBR Recursive Next Hop for IPv4 Traffic

The PBR Recursive Next Hop feature enables configuration of a recursive next-hop address in a PBR route map. The recursive next-hop address is installed in the routing table and can be a subnet that is not directly connected. If the recursive next-hop address is not available, traffic is routed using a default route.

Default Settings for PBR

None.

How to Configure PBR

- Configuring PBR
- Configuring Local PBR
- Configuring PBR Recursive Next Hop

Note For information about Multi-VRF Selection Using Policy Based Routing (PBR VRF), see this document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_mltvrf_slct_pbr.html

Configuring PBR

To configure PBR on an interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# route-map map-tag [permit | deny] [sequence-number]`	Defines a route map to control where packets are output. This command puts the router into route-map configuration mode.

Step 2	`Router(config-route-map)# match length min max`
	
	`Router(config-route-map)# match ip address {access-list-number | name} [...access-list-number | name]`
		Specifies the match criteria.
		
		Although there are many route-map matching options, here you can specify only length and/or ip address.
		
		• **length** matches the Level 3 length of the packet.
		• **ip address** matches the source or destination IP address that is permitted by one or more standard or extended access lists.
		
		If you do not specify a **match** command, the route map applies to *all* packets.

Step 3	`Router(config-route-map)# set ip precedence [number | name]`
	
	`Router(config-route-map)# set ip df`
	
	`Router(config-route-map)# set ip vrf vrf_name`
	
	`Router(config-route-map)# set ip next-hop ip-address [... ip-address]`
	
	`Router(config-route-map)# set ip next-hop recursive ip-address [... ip-address]`
	
	`Router(config-route-map)# set interface interface-type interface-number [... type number]`
	
	`Router(config-route-map)# set ip default next-hop ip-address [... ip-address]`
	
	`Router(config-route-map)# set default interface interface-type interface-number [... type ...number]`
		Specifies the action(s) to take on the packets that match the criteria. You can specify any or all of the following:
		
		• **precedence**: Sets precedence value in the IP header. You can specify either the precedence number or name.
		• **df**: Sets the 'Don't Fragment' (DF) bit in the ip header.
		• **vrf**: Sets the VPN Routing and Forwarding (VRF) instance.
		• **next-hop**: Sets next hop to which to route the packet.
		• **next-hop recursive**: Sets next hop to which to route the packet if the hop is to a router which is not adjacent.
		• **interface**: Sets output interface for the packet.
		• **default next-hop**: Sets next hop to which to route the packet if there is no explicit route for this destination.
		• **default interface**: Sets output interface for the packet if there is no explicit route for this destination.

	Command	Purpose
Step 4	`Router(config-route-map)# interface interface-type interface-number`	Specifies the interface, and puts the router into interface configuration mode.
Step 5	`Router(config-if)# ip policy route-map map-tag`	Identifies the route map to use for PBR. One interface can have only one route map tag; but you can have several route map entries, each with its own sequence number. Entries are evaluated in order of their sequence numbers until the first match occurs. If no match occurs, packets are routed as usual.

The **set** commands can be used in conjunction with each other. They are evaluated in the order shown in Step 3 in the previous task table. A usable next hop implies an interface. Once the local router finds a next hop and a usable interface, it routes the packet.

Configuring Local PBR

To configure PBR for all traffic that originates on the switch, perform this task:

Command	Purpose
`Router(config)# ip local policy route-map map-tag`	Identifies the route map to use for local PBR.

Note
- Local PBR traffic is processed in software on the RP.
- Use the **show ip local policy** command to display the route map used for local PBR.

Configuring PBR Recursive Next Hop

Setting the Recursive Next-Hop IP Address

Note PBR supports only one recursive next-hop IP address per route-map entry.

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list permit** *source* **Example:** `Router(config)# access-list 101 permit 10.60.0.0 0.0.255.255`	Configures an access list. The example configuration permits any source IP address that falls within the 10.60.0.0. 0.0.255.255 subnet.
Step 4	**route-map** *map-tag* **Example:** `Router(config)# route-map abccomp`	Enables policy routing and enters route-map configuration mode.
Step 5	**set ip next-hop** *ip-address* **Example:** `Router(config-route-map)# set ip next-hop 10.10.1.1`	Sets a next-hop router IP address. **Note** Set this IP address separately from the next-hop recursive router configuration.
Step 6	**set ip next-hop** {*ip-address* [*...ip-address*] | **recursive** ip-address} **Example:** `Router(config-route-map)# set ip next-hop recursive 10.20.3.3`	Sets a recursive next-hop IP address. **Note** This configuration does not ensure that packets get routed using the recursive IP address if an intermediate IP address is a shorter route to the destination.
Step 7	**match ip address** *access-list-number* **Example:** `Router(config-route-map)# match ip address 101`	Sets an access list to be matched.
Step 8	**end** **Example:** `Router(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

Verifying the Recursive Next-Hop Configuration

To verify the recursive next-hop configuration, perform the following steps.

Step 1 **show running-config | begin abccomp**

Use this command to verify the IP addresses for a next-hop and recursive next-hop IP address, for example:

```
Router# show running-config | begin abccomp

route-map abccomp permit 10
 match ip address 101 ! Defines the match criteria for an access list.
 set ip next-hop recursive 10.3.3.3 ! If the match criteria are met, the recursive IP
 address is set.
 set ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
```

Step 2 **show route-map** *map-name*

Use this command to display the route maps, for example:

```
Router# show route-map abccomp

route-map abccomp, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip next-hop recursive 10.3.3.3
  ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
 Policy routing matches: 0 packets, 0 bytes
```

Configuration Examples for PBR

Note The examples shown below involve the use of the **access-list** command (ACL). The log keyword should not be used with this command in policy-based routing (PBR) because logging is not supported at the interrupt level for ACLs.

Equal Access Example

The following example provides two sources with equal access to two different service providers. Packets arriving on asynchronous interface 1 from the source 209.165.200.225 are sent to the router at 209.165.200.228 if the router has no explicit route for the destination of the packet. Packets arriving from the source 209.165.200.226 are sent to the router at 209.165.200.229 if the router has no explicit route for the destination of the packet. All other packets for which the router has no explicit route to the destination are discarded.

```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
interface async 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 209.165.200.228
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 209.165.200.229
```

```
route-map equal-access permit 30
 set default interface null0
```

Differing Next Hops Example

The following example illustrates how to route traffic from different sources to different places (next hops), and how to set the Precedence bit in the IP header. Packets arriving from source 209.165.200.225 are sent to the next hop at 209.165.200.227 with the Precedence bit set to priority; packets arriving from source 209.165.200.226 are sent to the next hop at 209.165.200.228 with the Precedence bit set to critical.

```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
interface ethernet 1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 209.165.200.227
!
route-map Texas permit 20
 match ip address 2
 set ip precedence critical
 set ip next-hop 209.165.200.228
```

Recursive Next-Hop IP Address: Example

The following example shows the configuration of IP address 10.3.3.3 as the recursive next-hop router:

```
route-map abccomp
 set ip next-hop 10.1.1.1
 set ip next-hop 10.2.2.2
 set ip next-hop recursive 10.3.3.3
 set ip next-hop 10.4.4.4
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum