CHAPTER 35

# Configuring Policy-Based Routing

This chapter describes the tasks for configuring policy-based routing (PBR) on a router and includes these major sections:



**Note** For complete syntax and usage information for the switch commands used in this chapter, look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

If the command is not found inthe Catalyst 4500 Command Reference, it will be found in the larger Cisco IOS library. Refer to the *Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

**Note** To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release.

## Overview of Policy-Based Routing

This section contains the following subsections:



PBR gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, lessening reliance on routes derived from routing protocols. To this end, PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.

You can set up PBR as a way to route packets based on configured policies. For example, you can implement routing policies to allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets.

PBR allows you to perform the following tasks:

- Classify traffic based on extended access list criteria. Access lists, then establish the match criteria.
- Route packets to specific traffic-engineered paths.

Policies can be based on IP address, port numbers, or protocols. For a simple policy, you can use any one of these descriptors; for a complicated policy, you can use all of them.

# Understanding PBR

All packets received on an interface with PBR enabled are passed through enhanced packet filters known as route maps. The route maps used by PBR dictate the policy, determining to where the packets are forwarded.

Route maps are composed of statements. The route map statements can be marked as permit or deny, and they are interpreted in the following ways:

- If a statement is marked as deny, the packets meeting the match criteria are sent back through the normal forwarding channels and destination-based routing is performed.
- If the statement is marked as permit and a packet matches the access-lists, then the first valid set clause is applied to that packet.

You specify PBR on the incoming interface (the interface on which packets are received), not outgoing interface.

## Understanding PBR on Supervisor Engine 6-E

The Catalyst 4500 Supervisor Engine 6-E supports matching route-map actions with a packet by installing entries in the TCAM that match the set of packets described by the ACLs in the match criteria of the route map. These TCAM entries point at adjacencies that either perform the necessary output actions or forward the packet to software if either hardware does not support the action or its resources are exhausted.

**Note** The scale of hardware-based PBR is determined by TCAM size and the time required for the CPU to flatten the ACL before programming into hardware. The later will noticeably increase if a PBR policy requires a considerable number of class-maps. For example, a PBR policy of 1,200 class-maps may require 60-90 minutes of "flatten" time before programming into hardware. This process may repeat if an adjacency change requires PBR reprogramming.

**Note** Packets matching a PBR policy and specified with **set interface** and/or **set default interface** actions are software switched and forwarded at the CEF forwarding rate.

## Understanding PBR Flow Switching

**Note** The Supervisor Engine 6-E does not implement PBR using flow switching.

The Catalyst 4500 switching engine supports matching a "set next-hop" route-map action with a packet on a permit ACL. All other route-map actions, as well as matches of deny ACLs, are supported by a flow switching model. In this model, the first packet on a flow that matches a route-map is delivered to the software for forwarding. Software determines the correct destination for the packet and installs an entry into the TCAM so that future packets on that flow are switched in hardware. The Catalyst 4500 switching engine supports a maximum of 4096 flows.

## Using Policy-Based Routing

You can enable PBR to change the routing path of certain packets from the obvious shortest path. For example, PBR can be used to provide the following functionality:

- equal access
- protocol-sensitive routing
- source-sensitive routing
- routing based on interactive versus batch traffic
- routing based on dedicated links

Some applications or traffic can benefit from source-specific routing; for example, you can transfer stock records to a corporate office on a higher-bandwidth, higher-cost link for a short time while sending routine application data, such as e-mail, over a lower-bandwidth, lower-cost link.

**Note** PBR configuration is only allowed on interfaces belonging to the global routing table. Else, the global VRF. policy cannot be attached to a VRF-aware interface.

# Policy-Based Routing Configuration Task List

To configure PBR, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining sections are optional. See the end of this chapter for the section "Policy-Based Routing Configuration Examples."

- Enabling PBR (Required)
- Enabling Local PBR (Optional)

## Enabling PBR

To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then you must enable PBR for that route map on a particular interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

To enable PBR on an interface, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch(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** | `Switch(config-route-map)# match ip address {access-list-number \| name} [...access-list-number \| name]` | Specifies the match criteria. Matches the source and destination IP address that is permitted by one or more standard or extended access lists. |
| Perform Step 3, 4, 5, or 6 | | |
| **Step 3** | `Switch(config-route-map)# set ip next-hop ip-address [... ip-address]` | Specifies the action or actions to take on the packets that match the criteria.<br>Specifies the next hop for which to route the packet (the next hop must be adjacent). This behavior is identical to a next hop specified in the normal routing table. |
| | Or | |
| **Step 4** | `Switch(config-route-map)# set interface interface-type interface-number [... type number]` | Specifies the action or actions to take on the packets that match the criteria.<br>Sets output interface for the packet. This action specifies that the packet is forwarded out of the local interface. The interface must be a Layer 3 interface (no switchports), and the destination address in the packet must lie within the IP network assigned to that interface. If the destination address for the packet does not lie within that network, the packet is dropped. |
| | Or | |
| **Step 5** | `Switch(config-route-map)# set ip default next-hop ip-address [... ip-address]` | Specifies the action or actions to take on the packets that match the criteria.<br>Sets next hop to which to route the packet if there is no explicit route for this destination. Before forwarding the packet to the next hop, the switch looks up the packet's destination address in the unicast routing table. If a match is found, the packet is forwarded by way of the routing table. If no match is found, the packet is forwarded to the specified next hop. |
| | Or | |
| **Step 6** | `Switch(config-route-map)# set default interface interface-type interface-number [...type ...number]` | Specifies the action or actions to take on the packets that match the criteria.<br>Sets output interface for the packet if there is no explicit route for this destination. Before forwarding the packet to the next hop, the switch looks up the packet's destination address in the unicast routing table. If a match is found, the packet is forwarded via the routing table. If no match is found, the packet is forwarded to the specified output interface. If the destination address for the packet does not lie within that network, the packet is dropped. |

| | Command | Purpose |
|---|---|---|
| **Step 7** | `Switch(config-route-map)# interface interface-type interface-number` | Specifies the interface. This command puts the router into interface configuration mode. |
| **Step 8** | `Switch(config-if)# ip policy route-map map-tag` | Identifies the route map to use for PBR. One interface can only have one route map tag, but you can have multiple route map entries with different sequence numbers. These entries are evaluated in sequence number order until the first match. If there is no match, packets are routed as usual. |

The **set** commands can be used in conjunction with each other. These commands 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.

## Enabling Local PBR

Packets that are generated by the router are not normally policy-routed. To enable local PBR for such packets, indicate which route map the router should use by performing this task:

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

All packets originating on the router are then be subject to local PBR.

Use the **show ip local policy** command to display the route map used for local PBR, if one exists.

## Unsupported Commands

The following PBR commands in config-route-map mode are in the CLI but not supported in Cisco IOS for the Catalyst 4500 series switches. If you attempt to use these commands, an error message displays.

- match-length
- set ip qos
- set ip tos
- set ip precedence

# Policy-Based Routing Configuration Examples

The following sections provide PBR configuration examples:

- Equal Access, page 35-6
- Differing Next Hops, page 35-6
- Deny ACE, page 35-6

For information on how to configure policy-based routing, see the section "Policy-Based Routing Configuration Task List" in this chapter.

# Equal Access

The following example provides two sources with equal access to two different service providers. Packets arriving on interface fastethernet 3/1 from the source 1.1.1.1 are sent to the router at 6.6.6.6 if the router has no explicit route for the destination of the packet. Packets arriving from the source 2.2.2.2 are sent to the router at 7.7.7.7 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.

```
Switch (config)# access-list 1 permit ip 1.1.1.1
access-list 1 permit ip 1.1.1.1
!
interface fastethernet 3/1
 ip policy route-map equal-access
!

route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 6.6.6.6
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 7.7.7.7
route-map equal-access permit 30
 set default interface null0
```

**Note** If the packets you want to drop do not match either of the first two route-map clauses, then change **| set default interface null0** to **set interface null0**.

# Differing Next Hops

The following example illustrates how to route traffic from different sources to different places (next hops). Packets arriving from source 1.1.1.1 are sent to the next hop at 3.3.3.3; packets arriving from source 2.2.2.2 are sent to the next hop at 3.3.3.5.

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 3/1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip next-hop 3.3.3.3
!
route-map Texas permit 20
 match ip address 2
 set ip next-hop 3.3.3.5
```

# Deny ACE

The following example illustrates how to stop processing a given route map sequence, and to jump to the next sequence. Packets arriving from source 1.1.1.1 skip sequence 10 and jump to sequence 20. All other packets from subnet 1.1.1.0 follow the set statement in sequence 10.

```
access-list 1 deny ip 1.1.1.1
access-list 1 permit ip 1.1.1.0 0.0.0.255
access-list 2 permit ip 1.1.1.1
```

```
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 3/1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip next-hop 3.3.3.3
!
route-map Texas permit 20
match ip address 2
set ip next-hop 3.3.3.5
```