Policy-Based Routing

Policy-based routing is a process whereby the device puts packets through a route map before routing them. The route map determines which packets are routed to which device next. You might enable policy-based routing if you want certain packets to be routed some way other than the obvious shortest path. Possible applications for policy-based routing are to provide equal access, protocol-sensitive routing, source-sensitive routing, routing based on interactive versus batch traffic, and routing based on dedicated links. Policy-based routing is a more flexible mechanism for routing packets than destination routing.

To enable policy-based routing, you must identify which route map to use for policy-based routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met.

To enable policy-based routing on an interface, indicate which route map the device should use by using the **ip policy route-map** *map-tag* command in interface configuration mode

To define the route map to be used for policy-based routing, use the **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] global configuration command.

Only **set ip next-hop** command can be used under route-map configuration mode when you configure policy-based routing.

To define the criteria by which packets are examined to learn if they will be policy-based routed, use the **match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*] command in route map configuration mode. No match clause in the route map indicates all packets.

Note Mediatrace will show statistics of incorrect interfaces with policy-based routing (PBR) if the PBR does not interact with CEF.

Note Management implications: Since the policy based routing alters the conventional path (learnt through routing protocols) the traffic would have taken, the policies should be defined in a deterministic manner to keep the network manageable without impacting running services or applications. For example, the policy based routing can alter the path for the control traffic and affect protocols like OSPF, multicast, etc. Hence the policies need to be defined considering these aspects.

Restrictions on the Policy-Based Routing

- ACL and PBR are not supported together on the same SVI. Only one of the access-group (permit or deny access list) or IP policy route-map can be configured on the same SVI.
- IPv6 PBR is not supported.
- FRR is not supported with PBR.
- PBR is supported only on the SVI interfaces. It is not supported on Physical ports, EFPs, and EVCs.
- Single route-map entry is supported for each **ip policy route-map** command usage instances. Multiple route-map sequence entries for the same route-map are not supported (route-map with multiple sequence of route-map-entries).
- Only the access list is supported as match clause. Prefix list and other match clauses are not supported.
- Only one ACL is supported for route-map entry match statement.
- Only one match statement is supported for each route-map entry.
- Only **set ip next-hop** command is supported for the route-map entry. The **set ip next-hop recursive** command is not supported. Consequently, the next-hop which is going to be MPLS path is not supported. Other set commands including **set ip vrf**, **set ip precedence** etc. are not supported.
- PBR is applicable for ingress traffic only and is not applicable for locally generated packets.
- IPv6 traffic filter and IPv4 PBR are not supported together on the same interface.
- One ACL can be associated to only one SVI interface (either through "IPv4 Policy Route-map" or through "IPv4 Access group") on one device.
- We recommend a maximum of 50 ACE rules in one access-List for all access-lists being used for PBR (route-map).

How to Configure Policy-Based Routing

Configuring ACLs

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list extended** *access-list-tag* **Example:** `Router(config)# ip access-list extended ACL1`	Defines an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations.
Step 4	**permit ip** *source-addr source-wildcard* **any** **Example:** `Router(config-ext-nacl)# permit ip 192.168.3.0 0.0.0.255 any`	Set conditions in named IP access list that permit packets. **Note** The 'deny' rules of access-list are ignored when the access-list is used for PBR purposes in a route-map.
Step 5	**end** **Example:** `Router(config-ext-nacl)# end`	Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure a Route-Map

Configuring Route-Map

Procedure

	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	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:**	Defines the conditions for redistributing routes from one routing protocol into another routing protocol or enables policy-based routing and enters route-map configuration mode.

	Command or Action	Purpose
	`Router(config)# route-map PBR1 permit 10`	
Step 4	**match ip address** *access-list-tag* **Example:** `Router(config-route-map)# match ip address ACL1`	Define the criteria by which packets are examined to learn if they will be policy-based routed.
Step 5	**set ip next-hop** *ip-address* **Example:** `Router(config-route-map)# set ip next-hop 30.30.30.3`	Specifies where to output packets that pass a match clause of a route map for policy routing.
Step 6	**end** **Example:** `Router(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

What to do next

Configure the IP Policy association (on SVI)

Configuring the IP Policy association (on SVI)

Procedure

	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	**interface** *type number* **Example:** `Router(config)# interface vlan 100`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address* **Example:**	Defines the IP address for the interface.

	Command or Action	Purpose
	`Router(config-if)# ip address 100.0.0.2 255.255.255.0`	
Step 5	**ip policy route-map** *route-map-tag* **Example:** `Router(config-if)# ip policy route-map PBR1`	Identifies a route map to use for policy routing on an interface..
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the PBR Configuration

To display the interfaces where PBR is enabled, use the show ip policy command as shown in the following example:

```
Router# show ip policy

Interface Route map
Vlan10 RMAP1
```

To display the route-map sequence configuration, use the show route-map command as shown in the following example:

```
Router# show route-map MAP1

route-map MAP1, permit, sequence 10
  Match clauses:
    ip address (access-lists): 100
  Set clauses:
    ip next-hop 192.168.40.1
  Policy routing matches: 0 packets, 0 bytes
```

Configuration Example for the Policy-Based Routing

```
Building configuration...

Current configuration : 13748 bytes
!
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
!
interface GigabitEthernet0/8
 no ip address
 negotiation auto
 no qos-config scheduling-mode min-bw-guarantee
 service instance 70 ethernet
  encapsulation dot1q 70
  rewrite ingress tag pop 1 symmetric
```

```
  bridge-domain 70
 !
 !
 !
!
interface Vlan221
 ip address 192.168.221.1 255.255.255.0
 ip policy route-map MAP1
 ip ospf 100 area 0
!
interface Vlan222
 ip address 192.168.222.1 255.255.255.0
 ip policy route-map MAP2
 ip ospf 100 area 0
!
interface Vlan246
!
router ospf 500
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 500
 network 192.168.40.0 0.0.0.255 area 500
 network 192.168.50.0 0.0.0.255 area 500
 network 192.168.60.0 0.0.0.255 area 500
 network 192.168.70.0 0.0.0.255 area 500
!
router ospf 100
!
router ospf 5090
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.77.224.1
!
access-list 100 permit ip host 12.12.12.1 host 20.20.20.1
access-list 200 permit ip host 11.11.111.1 host 10.10.10.1
!
route-map MAP1 permit 10
 match ip address 100
 set ip next-hop 192.168.40.1
!
route-map MAP2 permit 10
 match ip address 200
 set ip next-hop 192.168.50.1
!
tftp-server flash:asr901-universalk9-mz.5jan_mcp_hsrp
!
control-plane
!
environment monitor
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
exception crashinfo buffersize 128
!
!
end
```

Additional References

Related Documents

Related Topic	Document Title
IP routing protocol-independent commands	Cisco IOS IP Routing: Protocol-Independent Command Reference

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 Policy-Based Routing

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 Policy-Based Routing

Feature Name	Releases	Feature Information
Policy-Based Routing	Cisco IOS Release 15.5(2)S	This feature was introduced on the Cisco ASR 901 Series Routers.