# Configuring IPv4 Policy-Based Routing

- Information About Policy-Based Routing, on page 1
- Restrictions and Limitations for Policy-Based Routing, on page 2
- How to Configure PBR, on page 5

## Information About Policy-Based Routing

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

PBR (Policy Based Routing) is a technique used to make routing decisions based on configured policies.

When a router or switch receives a packet, a forwarding decision is based on the destination IP address of the packet, which is used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria, for example, the source IP address and not the destination IP address. This permits routing of packets originating from different sources to different networks, even when the destinations are the same, and can be useful when interconnecting several private networks.

With PBR, you classify traffic using access control lists (ACLs) and then make traffic go through a different path. PBR is applied to incoming packets. All packets received on an interface with PBR enabled are passed through route maps. Based on the criteria defined in the route maps, packets are forwarded (routed) to the appropriate next hop.

- Route map statement marked as permit is processed as follows:
    - A match command can match on multiple ACLs. A route map statement can contain multiple match commands. Logical or algorithm function is performed across all the match commands to reach a permit or deny decision.

      For example:

      match ip address acl1 acl2

      match ip address acl3

**Note** IPv6 is not supported.

A packet is permitted if it is permitted by acl1 or acl2 or acl3.

- If the decision reached is permit, then the action specified by the **set** command is applied on the packet.
- If the decision reached is deny, then the PBR action (specified in the **set** command) is not applied. Instead the processing logic moves forward to look at the next route-map statement in the sequence (the statement with the next higher sequence number). If no next statement exists, PBR processing terminates, and the packet is routed using the default IP routing table.

- For PBR, route-map statements and ACLs marked as deny are not supported.

You can use standard IP ACLs to specify match criteria for a source address or extended IP ACLs to specify match criteria based on an end station. The process proceeds through the route map until a match is found. If no match is found, normal destination-based routing occurs. There is an implicit deny at the end of the list of match statements.

If match clauses are satisfied, you can use a set clause to specify the IP addresses identifying the next hop router in the path. You can also set an IP precedence value using the precedence number or name.

# Restrictions and Limitations for Policy-Based Routing

- To use PBR, you must have the Network Advantage license enabled on the switch.
- By default, Policy-Based Routing (PBR) is DISABLED on the switch. PBR is enabled when a route-map is configured and applied on interface.
- Packets that are generated by the switch (CPU), or local packets, are not normally policy-routed. When you globally enable local PBR on the switch, all unicast packets that originate on the switch are subject to local PBR. The protocols that are supported for local PBR are NTP, DNS, MSDP, SYSLOG and TFTP. Local PBR is disabled by default.
- The switch does not support **route-map deny** statements for PBR.
- Match ACLs with deny ACEs not supported.
- When a policy route map is applied to a physical interface, that interface cannot become a member of an EtherChannel.
- VRF and PBR are mutually-exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface.
- When a policy route map is applied on an interface along with ACL and QoS, ACL and QoS have higher precedence.
- IP Source Guard has a higher precedence if a rule matches with the PBR rule on the same interface.
- On an SVI interface, IP Source Guard and PBR rules are merged based on requirements.
- Multicast traffic is not policy-routed. PBR applies only to unicast traffic.

- You can enable PBR on a routed port or an SVI.
- You can define a maximum of 64 IP policy route maps on the switch.
- You can define a maximum of 64 access control entries (ACEs) for PBR on the switch.
- The number of hardware entries used by PBR depends on the route map itself, the ACLs used, and the order of the ACLs and route-map entries. The maximum number of entries is 256.
- VRF and PBR are mutually exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. The reverse is also true, you cannot enable PBR when VRF is enabled on an interface.
- Web Cache Communication Protocol (WCCP) and PBR are mutually exclusive on a switch interface. You cannot enable WCCP when PBR is enabled on an interface. The reverse is also true, you cannot enable PBR when WCCP is enabled on an interface.
- PBR based on TOS, DSCP and IP Precedence are not supported.
- Set interface, set default next-hop and set default interface are not supported.
- **ip next-hop recursive** and **ip next-hop verify availability** features are not available and the next-hop should be directly connected.
- For a single sequence route-map only one set clause is supported at a time. For a route-map with multiple sequences only set clauses of the same type are allowed. For example, if **set ip next-hop** is used in the first sequence, then the second sequence should also have the same set clause **set ip next-hop**.
- Policy-maps with no set actions are supported. Matching packets are routed normally.
- Policy-maps with no match clauses are supported. Set actions are applied to all packets.

The following table summarizes the PBR support for ACL match field options on the switch.

*Table 1: PBR Supported ACL Match field Options*

| Match Field | Supported (Y/N) |
|---|---|
| Source IP address | Y |
| Destination IP address | Y |
| Next Header (ICMP, IGMP, etc.) | N |
| TCP/UDP Port | N |
| Type of Service (TOS) | N |
| Fragmentation Bit | N |

This table lists the PBR feature support on the switch.

*Table 2: PBR Feature Support*

| Feature | Support/Scale |
|---|---|
| PBR on Ingress Traffic | Y |
| PBR on Egress Traffic | N |

| Feature | Support/Scale |
|---|---|
| PBR on Physical Interface (L2 Port) | N |
| PBR on Physical Interface (Routed Port) | Y |
| PBR on SVI Interface | Y |
| PBR on Port Channel (L2) | N |
| PBR on Port Channel (L3) | N |
| PBR with VRF | N |
| Match on IPv4 ACL | Y<br>**Note** Refer to table above for PBR Supported ACL Match field Options. |
| Match on Extended/Standard IPv4 ACL | Y |
| Match Based on Packet Length | N |
| Match with DENY ACE | N |
| Action Set Fragment Bit | N |
| Action to Set Precedence | N |
| Action to Set Next-Hop | Y |
| Recursive Next-Hop Action | N |
| Action to Set Interface | N |
| Action to Set Default Interface | N |
| Action to Set IP Precedence | Y |
| Action to Set IP VRF | Y |
| Set IP default Next-Hop | N |
| Set IP Default VRF | N |
| PBR on Multicast Traffic | N |
| PBR on IPv6 Traffic | N |
| Route-Map Deny | N |
| MAX number of route-map supported | 64 |
| MAX number of ACL policies supported | 64 |
| Local PBR | Y |

# How to Configure PBR

By default, PBR is disabled on the switch. To enable PBR, you must create a route map that specifies the match criteria and the resulting action. Then, you must enable PBR for that route map on an interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

### Before you begin

Refer to Restrictions and Limitations for Policy-Based Routing, on page 2.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **route-map** *map-tag* [**permit**] [*sequence number*]<br>**Example:**<br>`Device(config)# route-map pbr-map permit` | Defines route maps that are used to control where packets are output, and enters route-map configuration mode.<br>• *map-tag* — A meaningful name for the route map. The **ip policy route-map** interface configuration command uses this name to reference the route map. Multiple route-map statements with the same map tag define a single route map.<br>• (Optional) **permit** — If **permit** is specified and the match criteria are met for this route map, the route is policy routed as defined by the set actions.<br>• (Optional) *sequence number* — The sequence number shows the position of the route-map statement in the given route map. |
| **Step 4** | **match ip address** {*access-list-number* \| *access-list-name*} [*access-list-number* \|...*access-list-name*]<br>**Example:**<br>`Device(config-route-map)# match ip address 110 140` | Matches the source and destination IP addresses that are permitted by one or more standard or extended access lists. ACLs can match on more than one source and destination IP address.<br>If you do not specify a **match** command, the route map is applicable to all packets. |
| **Step 5** | **set ip next-hop** *ip-address* [...*ip-address*]<br>**Example:**<br>`Device(config-route-map)# set ip next-hop 10.1.6.2` | Specifies the action to be taken on the packets that match the criteria. Sets next hop to which to route the packet (the next hop must be adjacent). |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **set ip vrf** *vrf-name* **next-hop** *ip-address* [*...ip-address*]<br>**Example:**<br>`Device(config-route-map)# set ip vrf myvrf next-hop 10.5.5.5` | Allows you to apply policy-based routing to a VRF interface. |
| **Step 7** | **set ip precedence** [*number* \| *name*]<br>**Example:**<br>`Device(config-route-map)# set ip precedence 5` | • 0—routine<br>• 1—priority<br>• 2—immediate<br>• 3—flash<br>• 4—flash-override<br>• 5—critical<br>• 6—internet<br>• 7—network<br>Sets the precedence value in the IP header. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-route-map)# exit` | Returns to global configuration mode. |
| **Step 9** | **interface** *interface-id*<br>**Example:**<br>`Device(config)# interface gigabitethernet 1/1` | Enters interface configuration mode, and specifies the interface to be configured. |
| **Step 10** | **ip policy route-map** *map-tag*<br>**Example:**<br>`Device(config-if)# ip policy route-map pbr-map` | Enables PBR on a Layer 3 interface, and identify the route map to use. You can configure only one route map on an interface. However, you can have multiple route map entries with different sequence numbers. These entries are evaluated in the order of sequence number until the first match. If there is no match, packets are routed as usual. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Returns to global configuration mode. |
| **Step 12** | **ip local policy route-map** *map-tag*<br>**Example:**<br>`Device(config)# ip local policy route-map local-pbr` | (Optional) Enables local PBR to perform policy-based routing on packets originating at the switch. This applies to packets generated by the switch, and not to incoming packets. |
| **Step 13** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 14** | **show route-map** [*map-name*]<br>**Example:**<br>`Device# show route-map` | (Optional) Displays all the route maps configured or only the one specified to verify configuration. |
| **Step 15** | **show ip policy**<br>**Example:**<br>`Device# show ip policy` | (Optional) Displays policy route maps attached to the interface. |
| **Step 16** | **show ip local policy**<br>**Example:**<br>`Device# show ip local policy` | (Optional) Displays whether or not local policy routing is enabled and, if so, the route map being used. |