Multi-VRF Selection Using Policy-Based Routing (PBR)

First Published: June 5, 2007
Last Updated: February 27, 2009

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature allows a specified interface on a provider edge (PE) router to route packets to Virtual Private Networks (VPNs) based on packet length or match criteria defined in an IP access list.

You can enable VPN routing and forwarding (VRF) selection by policy routing packets through a route map, through the global routing table, or to a specified VRF.

You can enable policy-routing packets for VRF instances by using route map commands with **set** commands.

This feature and the *Directing MPLS VPN Traffic Using a Source IP Address* feature can be configured together on the same interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Multi-VRF Selection Using Policy-Based Routing (PBR)" section on page 16.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Multi-VRF Selection Using Policy-Based Routing (PBR)

- The router must support policy-based routing (PBR) in order for you to configure this feature. For platforms that do not support PBR, use the *Directing MPLS VPN Traffic Using a Source IP Address* feature.
- A VRF must be defined before you configure this feature. An error message is displayed on the console if no VRF exists.

Restrictions for Multi-VRF Selection Using Policy-Based Routing (PBR)

- All commands that aid in routing also support hardware switching, except for the **set ip next-hop verify availability** command because Cisco Discovery Protocol information is not available in the line cards.
- Protocol Independent Multicast (PIM) and multicast packets do not support PBR and cannot be configured for a source IP address that is a match criterion for this feature.
- The **set vrf** and **set ip global next-hop** commands can be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. But the **set vrf** and **set ip global next-hop** commands take precedence over the **set default interface**, **set interface, set ip default next-hop**, and **set ip next-hop** commands. No error message is displayed if you attempt to configure the **set vrf** command with any of these three **set** commands.
- The Multi-VRF Selection Using Policy-Based Routing (PBR) feature cannot be configured with IP prefix lists.
- The **set global** and **set vrf** commands cannot be simultaneously applied to a route map.
- The Multi-VRF Selection Using Policy-Based Routing (PBR) feature supports VRF-lite; that is, only IP routing protocols run on the router. Multiprotocol Label Switching (MPLS) and VPN cannot be configured.

Information About Multi-VRF Selection Using Policy-Based Routing (PBR)

Before using the Multi-VRF Selection Using Policy-Based Routing (PBR) feature, you need to understand the following concepts:

Policy Routing of VPN Traffic Based on Match Criteria

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature is an extension of the VRF Selection Based on Source IP Address feature. The PBR implementation of the VRF selection feature allows you to policy route VPN traffic based on match criteria. Match criteria are defined in an IP access list or are based on packet length. The following match criteria are supported in Cisco IOS software:

- IP access lists—Define match criteria based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access list configuration options in Cisco IOS software can be used to define match criteria.
- Packet lengths—Define match criteria based on the length of a packet, in bytes. The packet length filter is defined in a route map with the **match length** route-map configuration command.

Policy routing is defined in the route map. The route map is applied to the incoming interface with the **ip policy route-map** interface configuration command. An IP access list is applied to the route map with the **match ip address** route-map configuration command. Packet length match criteria are applied to the route map with the **match length** route-map configuration command. The **set** action is defined with the **set vrf** route-map configuration command. The match criteria are evaluated, and the appropriate VRF is selected by the **set** command. This combination allows you to define match criteria for incoming VPN traffic and policy route VPN packets out to the appropriate VRF.

Policy-Based Routing set Commands

The following sections provide information about **set** commands:

Policy-routing Packets for VRF Instances

To enable policy-routing packets for VRF instances, you can use route map commands with the following **set** commands. They are listed in the order in which the router uses them during the routing of packets.

- **set tos**—Sets the Type of Service (TOS) bits in the header of an IP packet.
- **set df**—Sets the Don't Fragment (DF) bit in the header of an IP packet.
- **set vrf**—Routes packets through the specified interface. The destination interface can belong only to a VRF instance.
- **set global**—Routes packets through the global routing table. This command is useful for routing ingress packets belonging to a specific VRF through the global routing table.
- **set ip vrf next-hop**—Indicates where to output packets that pass a match criteria of a route map for policy routing when the next hop must be under a specified VRF.
- **set ip global next-hop**—Indicates where to forward packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS software uses the global routing table.

- **set interface**—When packets enter a VRF, routes the packets out of the egress interface under the same VRF according to the set interface policy, provided that the Layer 2 rewrite information is available.
- **set ip default vrf**—Provides inherit-VRF and inter-VRF routing. With inherit-VRF routing, packets arriving at a VRF interface are routed by the same outgoing VRF interface. With inter-VRF routing, packets arriving at a VRF interface are routed via any other outgoing VRF interface.
- **set ip default global**—Provides VRF to global routing.
- **set default interface**—Indicates where to output packets that pass a match criterion of a route map for policy routing and have no explicit route to the destination. The interface can belong to any VRF.
- **set ip global next-hop**—Routes packets through the global routing table, where the next hop lookup will be in the global routing table.
- **set ip default next-hop**—Indicates where to output packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

Change of Normal Routing and Forwarding Behavior

When you configure PBR, you can use the following four set commands to change normal routing and forwarding behavior. Configuring any of these set commands, with the potential exception of the set ip next-hop command, overrides the routing behavior of packets entering the interface if the packets do not belong to a VRF. The packets are routed from the egress interface across the global routing table.

- **set default interface**—Indicates where to output packets that pass a match criterion of a route map for policy routing and have no explicit route to the destination.
- **set interface**—When packets enter a VRF, routes the packets out of the egress interface under the same VRF according to the set interface policy, provided that the Layer 2 rewrite information is available.
- **set ip default next-hop**—Indicates where to output packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
- **set ip next-hop**—Indicates where to output packets that pass a match criterion of a route map for policy routing. If a packet is received on a VRF interface and is transmitted from another interface within the same VPN, the VRF context of the incoming packet will be inherited from the interface.

Support of Inherit-VRF, Inter-VRF, and VRF-to-Global Routing

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature supports inherit-VRF and inter-VRF. With inherit-VRF routing, packets arriving at a VRF interface are routed by the same outgoing VRF interface. With inter-VRF routing, packets arriving at a VRF interface are routed via any other outgoing VRF interface.

VRF-to-global routing causes packets that enter any VRF interface to be routed via the global routing table. When a packet arrives on a VRF interface, the destination lookup normally is done only in the corresponding VRF table. If a packet arrives on a global interface, the destination lookup is done in the global routing table.

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature modifies the following **set** commands to support inherit-VRF, inter-VRF, and VRF-to-global routing. The commands are listed in the order in which the router uses them during the routing of packets.

- **set vrf**—Selects the appropriate VRF after a successful match occurs in the route map. VRS-aware PSV allows only inter-VRF (or VRF-to-VRF) switching.

- **set global**—Routes packets through the global routing table. This command is useful for routing ingress packets belonging to a specific VRF through the global routing table.
- **set ip vrf next-hop**—Causes the router to look up the next hop in the VRF table. If a packet arrives on an interface that belongs to a VRF and the packet needs to be routed via a different VRF, you can use the **set ip vrf next-hop** command.
- **set ip global next-hop**—Indicates where to forward packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS software uses the global routing table.
- **set interface**—When packets enter a VRF, routes the packets out of the egress interface under the same VRF, according to the set interface policy, provided that the Layer 2 rewrite information is available.
- **set ip default vrf**—Provides inherit-VRF and inter-VRF routing. With inherit-VRF routing, packets arriving at a VRF interface are routed by the same outgoing VRF interface. With inter-VRF routing, packets arriving at a VRF interface are routed via any other outgoing VRF interface.
- **set default interface**—Indicates where to output packets that pass a match criterion of a route map for policy routing and have no explicit route to the destination. The interface can belong to any VRF.
- **set ip next-hop**—Routes packets through the global routing table in an IP-to-IP routing and forwarding environment.

How to Configure Multi-VRF Selection Using Policy-Based Routing (PBR)

This section contains the following tasks:

Configuring Multi-VRF Selection Using PBR with a Standard Access List

This procedure uses a standard access list. The access list defines the match criteria for the route map. The match criteria can be based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} [**source** *source-wildcard*] [**log**]

	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** *access-list-number* {**deny** | **permit**} [**source** *source-wildcard*] [**log**] **Example:** `Router(config)# access-list 40 permit source 192.168.1.0 0.0.0.255`	Creates an access list and defines the match criteria for the route map. • Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. You can use all IP access list configuration options in Cisco IOS software to define match criteria. • The example creates a standard access list numbered 40. This filter permits traffic from any host with an IP address in the 192.168.1.0/24 subnet.

Configuring Multi-VRF Selection Using PBR with a Named Extended Access List

This task uses a named extended access list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*]
4. [*sequence-number*] {**permit** | **deny**} *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator-value*] [**log**] [**time-range** *time-range-name*] [**fragments**]

DETAILED STEPS

	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	**ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*] **Example:** `Router(config)# ip access-list extended NAMEDACL`	Specifies the IP access list type and enters the corresponding access list configuration mode. • You can specify a standard, extended, or named access list.
Step 4	[*sequence-number*] {**permit** | **deny**} *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*][**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator-vaue*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Router(config-ext-nacl)# permit ip any any option any-options`	Defines the criteria for which the access list will permit or deny packets. • Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. You can use all IP access list configuration options in Cisco IOS software to define match criteria. • The example creates a named access list that permits any configured IP option.

Configuring Multi-VRF Selection in a Route Map

Incoming packets are filtered through the match criteria that are defined in the route map. After a successful match occurs, the **set vrf** command configuration determines the VRF through which the outbound VPN packets will be policy routed.

Prerequisites

You must define the VRF before you configure the route map; otherwise an error message appears on the console.

A receive entry must be added to the VRF selection table with the **ip vrf receive** command. If a **match** and **set** operation occurs in the route map but there is no receive entry in the local VRF table, the packet will be dropped if the packet destination is local.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **set ip vrf** *vrf-name* **next-hop** {*ip-address* [*... ip-address*] | **recursive** *ip-address*}

   or

   set ip next-hop recursive vrf *vrf-name ip-address* [*ip-address*]

   or

   set ip global next-hop *ip-address* [*ip-address*]
5. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}

   or

   match length *minimum-length maximum-length*
6. **end**

DETAILED STEPS

	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:** `Router(config)# route-map map1 permit 10`	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. • Enters route-map configuration mode.

	Command or Action	Purpose

Step 4	**set ip vrf** *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}
	
	or
	
	set ip next-hop recursive vrf *ip-address* [*ip-address*]
	
	or
	
	set ip global next-hop *ip-address* [*ip-address*]
	
	Example:
	`Router(config-route-map)# set ip vrf myvrf next-hop 10.5.5.5`
	
	or
	
	Example:
	`Router(config-route-map)# set ip next-hop recursive vrf 10.5.5.5`
	
	or
	
	Example:
	`Router(config-route-map)# set ip global next-hop 10.5.5.5`
		Indicates where to forward packets that pass a match clause of a route map for policy routing when the next hop must be under a specified VRF name.
		
		or
		
		Indicates which destination or next hop will be used for packets that pass the match criterion configured in the route map.
		
		or
		
		Indicates where to forward packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software uses the global routing table.

Step 5	**match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
	
	or
	
	match length *minimum-length maximum-length*
	
	Example:
	`Router(config-route-map)# match ip address 1`
	
	or
	
	Example:
	`Router(config-route-map)# match length 3 200`
		Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or a prefix list, or to and perform policy routing on matched packets. IP access lists are supported.
		
		• The example configures the route map to use standard access list 1 to define match criteria.
		
		or
		
		Specifies the Layer 3 packet length in the IP header as a match criterion in a class map.
		
		• The example configures the route map to match packets that are 3 to 200 bytes in length.

Step 6	**end** **Example:** `Router(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

Configuring Multi-VRF Selection Using PBR and IP VRF Receive on the Interface

Packets coming through an interface are policy-routed only when the route map is attached to the incoming interface with the **ip policy route-map** interface configuration command.

The source IP address must be added to the VRF selection table. VRF selection is a one-way (unidirectional) feature. It is applied to the incoming interface. If a **match** and **set** operation occurs in the route map but there is no receive entry in the local VRF table, the packet is dropped if the packet destination is local.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip vrf receive** *vrf-name*
6. **end**

DETAILED STEPS

	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* [*name-tag*] **Example:** `Router(config)# interface FastEthernet 0/1`	Configures an interface and enters interface configuration mode.
Step 4	**ip policy route-map** *map-tag* **Example:** `Router(config-if)# ip policy route-map map1`	Identifies a route map to use for policy routing on an interface. • The configuration example attaches the route map named map1 to the interface.

	Command or Action	Purpose
Step 5	**ip vrf receive** *vrf-name* **Example:** `Router(config-if)# ip vrf receive VRF-1`	Adds the IP addresses that are associated with an interface into the VRF table. • This command must be configured for each VRF that will be used for VRF selection.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Multi-VRF Selection Using PBR

To verify the configuration of the Multi-VRF Selection Using Policy-Based Routing (PBR) feature, perform the following steps. You can enter the commands in any order.

SUMMARY STEPS

1. **show ip access-list** [*access-list-number* | *access-list-name*]
2. **show route-map** [*map-name*]
3. **show ip policy**

DETAILED STEPS

Step 1 **show ip access-list** [*access-list-number* | *access-list-name*]

To verify the configuration of match criteria for PBR multi-VRF selection, use the **show ip access-list** command. The following **show ip access-list** command output displays three subnet ranges defined as match criteria in three standard access lists:

```
Router# show ip access-list

Standard IP access list 40
 10 permit 10.1.0.0, wildcard bits 0.0.255.255
Standard IP access list 50
 10 permit 10.2.0.0, wildcard bits 0.0.255.255
Standard IP access list 60
 10 permit 10.3.0.0, wildcard bits 0.0.255.255
```

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

Use this command to verify **match** and **set** commands within the route map:

```
Router# show route-map
```

To verify the route-map configuration, use the **show route-map** command. The output displays the match criteria and **set** action for each route-map sequence. The output also displays the number of packets and bytes that have been policy routed per each route-map sequence.

```
Router# show route-map map1

route-map map1, permit, sequence 10
Match clauses:
Set clauses:
 ip next-hop vrf myvrf 10.5.5.5  10.6.6.6  10.7.7.7
```

```
 ip next-hop global 10.8.8.8  10.9.9.9
Policy routing matches: 0 packets, 0 bytes

Router# show route-map map2

route-map map2, permit, sequence 10
Match clauses:
Set clauses:
 vrf myvrf
Policy routing matches: 0 packets, 0 bytes

Router# show route-map map3

route-map map3, permit, sequence 10
Match clauses:
Set clauses:
 global
Policy routing matches: 0 packets, 0 bytes
```

The following **show route-map** command displays output from the **set ip vrf next-hop** command:

```
Router(config)# route-map test
Router(config-route-map)# set ip vrf myvrf next-hop
Router(config-route-map)# set ip vrf myvrf next-hop 192.168.3.2
Router(config-route-map)# match ip address 255 101
Router(config-route-map)# end
Router# show route-map

route-map test, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip vrf myvrf next-hop 192.168.3.2
 Policy routing matches: 0 packets, 0 bytes
```

The following **show route-map** command displays output from the **set ip global** command:

```
Router(config)# route-map test
Router(config-route-map)# match ip address 255 101
Router(config-route-map)# set ip global next-hop 192.168.4.2
Router(config-route-map)# end
Router# show route-map

*May 25 13:45:55.551: %SYS-5-CONFIG_I: Configured from console by consoleout-map
route-map test, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip global next-hop 192.168.4.2
 Policy routing matches: 0 packets, 0 bytes
```

Step 3 show ip policy

To verify the PBR multi-VRF selection policy, use the **show ip policy** command:

```
Router# show ip policy
```

The following **show ip policy** command output displays the interface and associated route map that is configured for policy routing:

```
Router# show ip policy

Interface          Route map
Ethernet0/1        PBR-VRF-Selection
```

Configuration Examples for Multi-VRF Selection Using Policy-Based Routing (PBR)

This section contains the following configuration examples:

Defining the Match Criteria for Multi-VRF Selection Using PBR: Example

In the following example, three standard access lists are created to define match criteria for three different subnetworks. Any packets received on Ethernet interface 0/1 will be policy routed through the PBR-VRF-Selection route map to the VRF that is matched in the same route-map sequence. If the source IP address of the packet is part of the 10.1.0.0/24 subnet, VRF1 will be used for routing and forwarding.

```
access-list 40 permit source 10.1.0.0 0.0.255.255
access-list 50 permit source 10.2.0.0 0.0.255.255
access-list 60 permit source 10.3.0.0 0.0.255.255

route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF1
 !
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF2
 !
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF3
 !
interface Ethernet 0/1
 ip address 192.168.1.6 255.255.255.252
 ip vrf forwarding VRF4
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF1
 ip vrf receive VRF2
 ip vrf receive VRF3
```

Configuring Multi-VRF Selection in a Route Map: Example

The following example shows a **set ip vrf next-hop** command that applies policy-based routing to the VRF interface named myvrf and specifies that the IP address of the next hop is 192.168.3.2:

```
Router(config)# route-map map1 permit
Router(config)# set vrf myvrf
Router(config-route-map)# set ip vrf myvrf next-hop 192.168.3.2
Router(config-route-map)# match ip address 101
Router(config-route-map)# end
```

The following example shows a **set ip global** command that specifies that the router should use the next hop address 192.168.4.2 in the global routing table:

```
Router(config-route-map)# set ip global next-hop 192.168.4.2
```

Additional References

The following sections provide references related to the Multi-VRF Selection Using Policy-Based Routing (PBR) feature.

Related Documents

Related Topic	Document Title
IP access list commands	*Cisco IOS Security Command Reference*
How to set up an interface on a PE router to route packets to different MPLS VPNs based on the source IP address of the packet	*Directing MPLS VPN Traffic Using a Source IP Address*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Multi-VRF Selection Using Policy-Based Routing (PBR)

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Multi-VRF Selection Using Policy-Based Routing (PBR)

Feature Name	Releases	Feature Information
Multi-VRF Selection Using Policy-Based Routing (PBR)	12.2(33)SRB1 12.2(33)SXH1 12.4(24)T	The Multi-VRF Selection Using Policy-Based Routing (PBR) feature allows a specified interface on a provider edge (PE) router to route packets to VPNs based on packet length or match criteria defined in an IP access list. This feature and the *Directing MPLS VPN Traffic Using a Source IP Address* feature can be configured together on the same interface. In 12.2(33)SRB1, this feature was introduced. In 12.2(33)SXH1, support was added. The following commands were modified: **set ip global next-hop**, and **set ip vrf next-hop**. In 12.4(24)T, this feature was integrated.

Glossary

CE router—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

inherit-VRF routing—Packets arriving at a VRF interface are routed by the same outgoing VRF interface.

inter-VRF routing—Packets arriving at a VRF interface are routed via any other outgoing VRF interface.

IP—Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

PBR—policy-based routing. PBR allows a user to manually configure how received packets should be routed.

PE router—provider edge router. A router that is part of a service provider's network and that is connected to a CE router. It exchanges routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv1, or RIPv2.

VPN—Virtual Private Network. A collection of sites sharing a common routing table. A VPN provides a secure way for customers to share bandwidth over an ISP backbone network.

VRF—A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

VRF-lite—A feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs.