Multi-VRF Selection Using Policy Based Routing (PBR)

First Published: June 5, 2007
Last Updated: April 10, 2012

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 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 virtual route forwarding (VRF) instances by using route-map commands with the following **set** clauses:

- **set vrf**—Routes packets through a specified VRF instance. The router looks for the outgoing interface in the VRF table.
- **set ip vrf**—Causes the router to look up the next hop in the VRF table.
- **set global**—Routes packets through the global routing table. This command is useful when you want to route ingress packets belonging to a specific VRF through the global routing table.
- **set ip global**—Routes packets through the global routing table, where the next-hop lookup will be in the global routing table.

This feature and the VRF Selection Based on Source IP Address feature can be configured together on the same interface.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Multi-VRF Selection Using Policy Based Routing (PBR)" section on page 26.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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.

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

Contents

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

- The router must support PBR in order to configure this feature. For platforms that do not support PBR, use the VRF Selection Based on Source IP Address feature introduced in Cisco IOS Release 12.0(22)S.
- 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)

- VRF Select is supported only in Service Provider (-p-) images.
- 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** 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** 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 the above four set clauses.
- The Multi-VRF Selection Using Policy Based Routing 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 feature supports VRF-lite; that is, only IP routing protocols are running on the router. MPLS and VPN cannot be configured. However, the **set vrf** command will work in MPLS VPN scenarios.

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, page 3
- Policy Based Routing Set Clauses, page 3

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** clause. 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 Clauses

When configuring PBR, the following four **set** clauses can be used to change normal routing and forwarding behavior:

- **set default interface**
- **set interface**
- **set ip default next-hop**
- **set ip next-hop**

Configuring any of the above **set** clauses overwrites the normal routing and forwarding behavior of a packet.

The Multi-VRF Selection Using Policy Based Routing (PBR) feature introduces the fifth **set** clause that can be used to change normal routing and forwarding behavior. The **set vrf** command is used to select the appropriate VRF after a successful match occurs in the route map.

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

This section contains the following procedures:

- Defining the Match Criteria for Multi-VRF Selection Using PBR, page 4
- Configuring Multi-VRF Selection in a Route Map, page 6
- Configuring Multi-VRF Selection Using PBR on the Interface, page 8
- Configuring IP VRF Receive on the Interface, page 9
- Verifying the Configuration of Multi-VRF Selection Using PBR, page 10

Defining the Match Criteria for Multi-VRF Selection Using PBR

The match criteria for multi-VRF selection using PBR are defined in an access list. Standard and named access lists are supported. The following sections explain how to configure PBR route selection:

- Configuring Multi-VRF Selection Using PBR with a Standard Access List, page 4
- Configuring Multi-VRF Selection Using PBR with a Named Access List, page 5

Match criteria can also be defined based on the packet length by configuring the **match length** route-map configuration command. This configuration option is defined entirely within a route map.

Prerequisites

The tasks in the following sections assume that the VRF and associated IP address are already defined.

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

This procedure uses a standard access list.

SUMMARY STEPS

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

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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] **Example:** `Router(config)# access-list 40 permit 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 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.

Restrictions

- If an interface is associated with a VRF by configuring the **ip vrf forwarding** interface configuration command, you cannot also configure the same interface to use PBR with the **set vrf** route-map configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match ip address** {*acl-number* [*acl-number* ... | *acl-name* ...] | *acl-name* [*acl-name* ... | *acl-number* ...]}

   or

   match length *minimum-length maximum-length*
5. **set vrf** *vrf-name*
6. **set ip vrf** *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}

   or

   set ip global next-hop *ip-address* [*ip-address*]
7. **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 RED 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	**match ip address** {*acl-number* [*acl-number* ... | *acl-name* ...] | *acl-name* [*acl-name* ... | *acl-number* ...]}
	Example:
	`Router(config-route-map)# match ip address 1`
	or
	match length *minimum-length maximum-length*
	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, and performs 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 between 3 and 200 bytes in size.

Step 5	**set vrf** *vrf-name* **Example:** `Router(config-route-map)# set vrf RED`	Enables VRF selection by policy-routing packets through a route map. • The example policy-routes matched packets out to the VRF named RED.

Step 6	**set ip vrf** *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}
	Example:
	`Router(config-route-map)# set ip vrf myvrf next-hop 10.5.5.5`
	or
	set ip global next-hop *ip-address* [*ip-address*]
	Example:
	`Router(config-route-map)# set ip global next-hop 10.5.5.5`
		Indicates where to output packets that pass a match clause of a route map for policy routing when the next hop must be under a specified VRF.
		or
		Indicates where to output 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 7	**end**
	Example:
	`Router(config-route-map)# end`
		Exits route-map configuration mode and returns to privileged EXEC mode.

Configuring Multi-VRF Selection Using PBR on the Interface

The route map is attached to the incoming interface with the **ip policy route-map** interface configuration command.

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 RED`
		Identifies a route map to use for policy routing on an interface.
		• The configuration example attaches the route map named RED to the interface.

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.

Configuring IP VRF Receive on the Interface

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(confif-if)# ip policy route-map wether`
		Identifies a route map to use for policy routing on an interface.

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. You must specify this command for each VRF that will be used for VRF selection.

Step 6	**`end`**
	Example:
	`Router(config-int)# 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.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip access-list** [*access-list-number* | *access-list-name*] **Example:** Router# show ip access-list	Displays the contents of all current IP access lists. • Use this command to verify the match criteria that are defined in the access list. Both named and numbered access lists are supported.
Step 3	**show route-map** [*map-name*] **Example:** Router# show route-map	Displays all route maps configured or only the one specified. • Use this command to verify **match** and **set** clauses within the route map.
Step 4	**show ip policy** **Example:** Router# show ip policy	Displays the route map used for policy routing. • Use this command to display the route map and the associated interface.

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: Example, page 11
- Configuring Multi-VRF Selection in a Route Map: Examples, page 12
- Verifying Multi-VRF Selection Using Policy Based Routing: Examples, page 12

Defining the Match Criteria for Multi-VRF Selection: Example

In the following example, three standard access lists are created to define match criteria for three different subnets. 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, VRF_1 will be used for routing and forwarding.

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

route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF_1
 !
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF_2
 !
```

```
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF_3
 !
interface Ethernet0/1
 ip address 192.168.1.6 255.255.255.252
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF_1
 ip vrf receive VRF_2
 ip vrf receive VRF_3
```

Configuring Multi-VRF Selection in a Route Map: Examples

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

```
Router(config)# route-map RED permit
Router(config-route-map)# set ip vrf Pink next-hop 192.168.3.2
Router(config-route-map)# match ip address 101
```

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
```

Verifying Multi-VRF Selection Using Policy Based Routing: Examples

The following verification examples show defined match criteria and route-map policy configuration.

Verifying Match Criteria

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

```
Router# show ip access-lists

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
```

Verifying Route-Map Configuration

To verify 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 NH

route-map NH, permit, sequence 10
Match clauses:
Set clauses:
 ip next-hop vrf RED 5.5.5.5 6.6.6.6 7.7.7.7
 ip next-hop global 8.8.8.8 9.9.9.9
Policy routing matches: 0 packets, 0 bytes

Router# show route-map NH2
```

```
route-map NH2, permit, sequence 10
Match clauses:
Set clauses:
 vrf RED
Policy routing matches: 0 packets, 0 bytes

Router# show route-map NH3

route-map NH3, 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** command:

```
Router(config)# route-map test
Router(config-route-map)# set ip vrf Pink n
Router(config-route-map)# set ip vrf Pink next-hop 192.168.3.2
Router(config-route-map)# match ip addr 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 Pink 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 addr 255 101
Router(config-route-map)# set ip global n
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
```

Verifying PBR Multi-VRF Selection 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
```

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
Selection of the source IP address instead of the policy based routing approach used in this document	*MPLS VPN: VRF Selection Based on Source IP Address*
IP access list commands	*Cisco IOS IP Addressing Services Command Reference*, Release 12.2SR

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 Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **set ip global**
- **set ip vrf**
- **show route-map**

set ip global

To indicate 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, use the **set ip global** command in route-map configuration mode. To disable this feature, use the **no** form of this command.

set ip global next-hop *ip-address* [*...ip-address*]

no set ip global next-hop *ip-address* [*...ip-address*]

Syntax Description

next-hop *ip-address*	IP address of the next hop.

Command Default

The router uses the next-hop address in the global routing table.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.

Usage Guidelines

Use this command to allow packets to enter a VRF interface and be policy-routed or forwarded out of the global table.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Examples

The following example allows use of the global table and specifies that the next-hop address is 10.5.5.5:

```
set ip global next-hop 10.5.5.5
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.

Command	Description
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip vrf	Indicates where to output packets that pass a match clause of a route map for policy routing when the next hop must be under a specified VRF name.

set ip vrf

To indicate 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 virtual route forwarding (VRF) name, use the **set ip vrf** command in route-map configuration mode. To disable this feature, use the **no** form of this command.

set ip vrf *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}

no set ip vrf *vrf-name* **next-hop** {*ip-address* [... *ip-address*] | **recursive** *ip-address*}

Syntax Description

vrf-name	Name of the VRF.
next-hop *ip-address*	IP address of the next hop to which packets are forwarded. The next hop must be an adjacent router.
next-hop recursive *ip-address*	IP address of the recursive next-hop router. **Note** The next-hop IP address must be assigned separately from the recursive next-hop IP address.

Command Default

The next hop does not have to be under a specified VRF.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.

Usage Guidelines

The **set ip vrf** command allows you to apply policy based routing to a VRF interface.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and **match** configuration commands to define the conditions for policy-routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which policy routing occurs. The **set** commands specify the set actions—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip vrf** command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. set TOS
2. set DF (Don't Fragment) bit in IP header
3. set vrf
4. set ip next-hop

5. set interface
6. set ip default next-hop
7. set default interface

Examples

The following example specifies that the next hop must be under the VRF name that has the IP address 10.5.5.5:

```
set ip vrf myvrf next-hop 10.5.5.5
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause 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 clause of a route map for policy routing.

show route-map

To display static and dynamic route maps, use the **show route-map** command in privileged EXEC mode.

show route-map [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**]

Syntax Description

map-name	(Optional) Name of a specific route map.
dynamic	(Optional) Displays dynamic route map information.
dynamic-map-name	(Optional) Name of a specific dynamic route map.
application	(Optional) Displays dynamic route maps based on applications.
application-name	(Optional) Name of a specific application.
all	(Optional) Displays all static and dynamic route maps.
detailed	(Optional) Displays the details of the access control lists (ACLs) that have been used in the **match** clauses for dynamic route maps.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for continue clauses was integrated into the command output.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	An additional counter collect policy routing statistic was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	Support for continue clauses was integrated into Cisco IOS Release 12.3(2)T.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(7)T	The **dynamic**, **application**, and **all** keywords were added.
12.0(28)S	The support for recursive next-hop clause was added.
12.3(14)T	The support for recursive next-hop clause was integrated into Cisco IOS Release 12.3(14)T. Support for the map display extension functionality was added. The **detailed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(31)SRB1	The command output shows global routing table information.

Usage Guidelines

For Cisco IOS Release 12.3(14)T and later 12.4 and 12.4T releases, you can display the ACL-specific information that pertains to the route map in the same display without having to execute a **show route-map** command to display each ACL that is associated with the route map.

Examples

The **show route-map** command will display configured route-maps, match, set, and continue clauses. The output will vary depending on which keywords are included with the command, and which software image is running in your router.

show route-map Command with No Keywords Specified Example

The following is sample output from the **show route-map** command:

```
Router# show route-map

route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, deny, sequence 40
  Match clauses:
    community (community-list filter): 20:2
  Set clauses:
    local-preference 100
  Policy routing matches: 0 packets, 0 bytes
route-map LOCAL-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

The following example shows Multiprotocol Label Switching (MPLS)-related route map information:

```
Router# show route-map

route-map OUT, permit, sequence 10
Match clauses:
  ip address (access-lists): 1
Set clauses:
  mpls label
Policy routing matches: 0 packets, 0 bytes

route-map IN, permit, sequence 10
Match clauses:
  ip address (access-lists): 2
  mpls label
Set clauses:
Policy routing matches: 0 packets, 0 bytes
```

Table 1 describes the significant fields shown in the display.

Table 1 show route-map Field Descriptions

Field	Description
route-map ROUTE-MAP-NAME	Name of the route map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses: tag	Match criteria—conditions under which redistribution is allowed for the current route map.
Continue:	Continue clause—shows the configuration of a continue clause and the route-map entry sequence number that the continue clause will go to.
Set clauses: metric	Set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met.
Policy routing matches:	Number of packets and bytes that have been filtered by policy routing.

show route-map Command with Dynamic Route Map Specified Example

The following is sample output from the **show route-map** command when entered with the **dynamic** keyword:

```
Router# show route-map dynamic

route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 0, identifier 1137954548
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 1, identifier 1137956424
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 2, identifier 1124436704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.1
    ip gateway 172.16.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

The following is sample output from the **show route-map** command when entered with the **dynamic** and **application** keywords:

```
Router# show route-map dynamic application

Application - AAA
  Number of active routemaps = 1
```

When you specify an application name, only dynamic routes for that application are shown. The following is sample output from the **show route-map** command when entered with the **dynamic** and **application** keywords and the AAA application name:

```
Router# show route-map dynamic application AAA

AAA
  Number of active rmaps = 2
AAA-02/06/04-14:01:26.619-1-AppSpec
AAA-02/06/04-14:34:09.735-2-AppSpec

Router# show route-map dynamic AAA-02/06/04-14:34:09.735-2-AppSpec

route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 0, identifier 1128046100
  Match clauses:
    ip address (access-lists): PBR#7 PBR#8
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 1, identifier 1141277624
  Match clauses:
    ip address (access-lists): PBR#9 PBR#10
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 2, identifier 1141279420
  Match clauses:
    ip address (access-lists): PBR#11 PBR#12
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.12
    ip gateway 172.16.1.12
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 2
```

show route-map Command with Detailed ACL Information for Route Maps Specified Example

The following is sample output from the **show route-map** command with the **dynamic** and **detailed** keywords entered:

```
Router# show route-map dynamic detailed

route-map AAA-01/20/04-22:03:10.799-1-AppSpec, permit, sequence 1, identifier 29675368
Match clauses:
ip address (access-lists):
Extended IP access list PBR#3
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Extended IP access list PBR#4
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Set clauses:
ip next-hop 172.16.1.14
ip gateway 172.16.1.14
Policy routing matches: 0 packets, 0 bytes
```

show route-map Command with Global Routing Table Information

The following is sample output from the **show route-map** command when the **set ip global** command has been specified:

```
route-map test
match ip addr 255 101
set ip global n
set ip global next-hop 192.168.4.2
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
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set ip global	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.

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

Table 2 lists the release history for this feature.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/cfn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

Table 2 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	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 VRF Selection Based on Source IP Address feature can be configured together on the same interface.

Glossary

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

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.