MPLS VPN: VRF Selection Using Policy Based Routing

First Published: March 1, 2004
Last Updated: February 19, 2007

The MPLS VPN: VRF Selection Using Policy Based Routing feature is an extension of the MPLS VPN: VRF Selection Based on Source IP Address feature. This feature introduces a policy-based routing (PBR) mechanism to classify and forward Virtual Private Network (VPN) traffic based on multiple VPN routing and forwarding (VRF) selection match criteria.

Feature History for the MPLS VPN: VRF Selection Using Policy Based Routing Feature

Release	Modification
12.3(7)T	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRB	This feature was integrated into Cisco IOS Release 12.2(33)SRB.

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.

Contents

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

Prerequisites for VRF Selection Using Policy Based Routing

- The router must support PBR 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 prior to the configuration of this feature. An error message is displayed on the console if no VRF exists.
- This document assumes that multiprotocol BGP (mBGP), Multiprotocol Label Switching (MPLS), and Cisco Express Forwarding are enabled in your network.

Restrictions for VRF Selection Using Policy Based Routing

- VRF Select is supported only in Service Provider (-p-) images.
- The VRF Selection Using Policy Based Routing feature can coexist with the VRF Selection Based on Source IP address feature on the same router, but these features cannot be configured together on the same interface. This is designed behavior to prevent VRF table selection conflicts that could occur if these features were misconfigured together. An error message is displayed on the console if you attempt to configure the **ip vrf select source** and the **ip vrf policy-map** commands on the same interface.
- Protocol Independent Multicast (PIM) and multicast packets do not support PBR and cannot be configured for a source IP address that is match criteria 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 four **set** commands.
- The VRF Selection Using Policy Based Routing feature cannot be configured with IP prefix lists.

VRF Selection Using Policy Based Routing

The VRF Selection Using Policy Based Routing 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 is defined in an IP access list or based on packet length. The following match criteria is 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 is 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 is 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: Overview

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 will overwrite normal routing forwarding behavior of a packet.

The VRF Selection Using Policy Based Routing 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 the successful match occurs in the route map. However, the **set vrf** command cannot be configured with the above four PBR set clauses. This is designed behavior, as we do not allow a packet to be set to an interface or a specific next hop when it is configured within a VRF. An error message will be displayed in the console if you attempt to configure the **set vrf** command with any of the above four PBR set clauses within the same route map.

How to Configure VRF Selection Using Policy Based Routing

This section contains the following procedures:

Defining the Match Criteria for PBR VRF Selection

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

Match Criteria Can Also Be Defined Based on Packet Length

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 PBR VRF Selection with a Standard Access List

This example uses a standard access list entered using the standard CLI.

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. All IP access list configuration options in Cisco IOS software can be used to define match criteria. • The example creates a standard access list numbered 40. This filter will permit traffic from any host with an IP address in the 192.168.1.0/24 subnet.

Configuring PBR VRF Selection with a Named Access List

This task uses a named extended access list that uses the named access-list configuration mode CLI.

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*] [**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. • A standard, extended, or named access list can be used.
Step 4	[*sequence-number*] **permit** | **deny protocol** *source source-wildcard* **destination** *destination-wildcard* [**option** *option-value*][**precedence** *precedence*] [**tos** *tos*] [**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. All IP access list configuration options in Cisco IOS software can be used to define match criteria. • The example creates a named access list that permits any configured IP option.

Configuring PBR 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

- The VRF must be defined prior to the configuration of the route map; otherwise an error message is displayed 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.
- This **set vrf** command cannot be configured with the **set ip default next-hop**, **set ip next-hop**, **set ip default interface**, and **set ip interface** route-map configuration commands. This is designed behavior, because we do not allow the interface to be set or allow the next hop to be changed when PBR VRF selection is enabled.

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. **exit**

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.

	Command or Action	Purpose
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.
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 criteria 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`	Defines which VRF to output VPN packets that are successfully matched in the same route map sequence for PBR VRF selection. • The example policy routes matched packets out to the VRF named RED.
Step 6	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and enters global configuration mode.

Configuring PBR on the Interface

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

Restrictions

- The VRF Selection Using Policy Based Routing feature can coexist with the VRF Selection Based on Source IP address feature on the same router, but the two features cannot be configured together on the same interface. This is designed behavior to prevent VRF table selection conflicts that could occur if these features were misconfigured together. An error message is displayed on the console if you attempt to configure the **ip vrf select source** and the **ip vrf policy-map** commands on the same interface.
- PBR can be configured on an interface where a VRF is defined. However, one of the following warning messages is displayed on the console if you attempt to configure both PBR and a VRF on the same interface:

```
%% Policy Based Routing is NOT supported for VRF" interfaces
%% IP-Policy can be used ONLY for marking "(set/clear DF bit) on
```

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. **exit**

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-int)# 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-int)# 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	**exit** **Example:** `Router(config-int)# exit`	Exits interface configuration mode and enters global configuration 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 will be 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	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 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 5	**end** **Example:** `Router(config-int)# end`	Exits interface configuration mode, and enters privileged EXEC mode.

Verifying the Configuration of the VRF Selection Using Policy Based Routing

To verify the configuration of the VRF Selection Using Policy Based Routing feature, perform the steps in this section.

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. • This command is used 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. • This command is used 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. • This command can be used to display the route map and the associated interface.

Configuration Examples for VRF Selection Using Policy Based Routing

This section provides the following configuration examples:

- PBR VRF Selection Defined in Access List: Example, page 11
- Verifying VRF Selection Using Policy Based Routing: Example, page 12

PBR VRF Selection Defined in Access List: Example

In the following example, three standard access lists are created to define match criteria for three different subnets. Any packets received on the Ethernet 0/1 interface 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
```

Verifying VRF Selection Using Policy Based Routing: Example

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 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

route-map PBR-VRF-Selection, permit, sequence 10
  Match clauses:
    ip address (access-lists): 40
  Set clauses:
    vrf VRF_1
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 20
  Match clauses:
    ip address (access-lists): 50
  Set clauses:
    vrf VRF_2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 30
  Match clauses:
    ip address (access-lists): 60
  Set clauses:
    vrf VRF_3
  Policy routing matches: 0 packets, 0 bytes
```

Verifying PBR 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 MPLS VPN—VRF Selection Using Policy Based Routing feature.

Related Documents

Related Topic	Document Title
The *MPLS VPN—VRF Selection Based on Source IP Address* document provides similar functionality implemented with an approach based on the 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 configuration is documented in the Cisco IOS IP Addressing Services Configuration Guide	*Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4 *Cisco IOS IP Configuration Guide*, Release 12.2SB
IP access list commands are documented in the Cisco IOS IP Addressing Services Command Reference	*Cisco IOS IP Addressing Services Command Reference*, Release 12.4T *Cisco IOS IP Addressing Services Command Reference*, Release 12.2 SR *Cisco IOS IP Command Reference*, Volume 1 of 3: Addressing and Services, Release 12.2
Route-map configuration is documented in the "Configuring BGP" chapter of the *Cisco IOS IP Configuration Guide*. Route-map configuration commands are documented in the *Cisco IOS IP Command reference*.	*Cisco IOS BGP Configuration Guide*, Release 12.4 *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T

Standards

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

MIBs

MIBs	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

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This feature uses no new or modified commands.

- **ip vrf receive**
- **set vrf**

ip vrf receive

To insert the IP address of an interface as a connected route entry in a Virtual Private Network (VPN) routing and forwarding instance (VRF) routing table, use the **ip vrf receive** command in interface configuration mode. To remove the connected entry from the VRF routing table, use the **no** form of this command.

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF into which you want to add the IP address of the interface.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip vrf receive** command supports VRF route selection for the following features:

- MPLS VPN: VRF Selection Based on Source IP Address
- MPLS VPN: VRF Selection Using Policy-Based Routing

This command is used to install a primary or secondary IP address of an interface as a connected route entry in the VRF routing table. These entries appear as "receive" entries in the Cisco Express Forwarding table. MPLS VPNs require CEF switching to make IP destination prefix-based switching decisions. This command can be used to selectively install the interface IP address in the VRF that is specified with the *vrf-name* argument. Only the local interface IP address is added to the VRF routing table. This command is used on a per-VRF basis. In other words, you must enter this command for each VRF in which you need to insert the IP address of the interface. This command does not remove the interface IP address from the global routing table.

Note This command cannot be used with the **ip vrf forward** command for the same interface.

VRF Selection Based on Source IP Address Guidelines

The **ip vrf receive** command is automatically disabled when the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner. Interfaces where the VRF Selection Based on Source IP Address feature is enabled can forward packets that have an IP address that corresponds to an IP address entry in the VRF table. If the VRF table does not contain a matching IP address, the packet is dropped, by default, because there is no corresponding "receive" entry in the VRF entry.

VRF Selection Using Policy Based Routing Guidelines

You must enter the **ip policy route-map** command before the **ip vrf receive** command can be enabled. The **ip vrf receive** command is automatically disabled when either the **no ip policy route-map** *map-name* or the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner. With the VRF Selection Using Policy-Based Routing implementation of the VRF selection feature, a route map filters the VRF routes. 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.

Examples

VRF Selection Based on Source IP Address

The following example shows how to configure Ethernet interface 0/2 (172.16.1.3) and insert its IP address in VRF_1 and VRF_2 with the **ip vrf receive** command. You must enter the **ip vrf select source** command on the interface or subinterface to enable VRF selection on the interface or subinterface. You must also enter the **vrf selection source** command in global configuration mode to populate the VRF selection table and to configure the VRF Selection Based on Source IP Address feature. (The **vrf selection source** command is not shown in this example.)

```
Router(config)# interface Ethernet0/2
Router(config-if)# ip address 172.16.1.3 255.255.255.255
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive VRF_1
Router(config-if)# ip vrf receive VRF_2
Router(config-if)# end
```

VRF Selection Using Policy-Based Routing

The following example shows how to configure Ethernet interface 0/1 (192.168.1.2) and insert its IP address in VRF_1 and VRF_2 with the **ip vrf receive** command. You must configure an access list and a route map to allow the VRF Section Using Policy-Based Routing feature to select a VRF. (The access list and route map configuration are not shown in this example.)

```
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.255
Router(config-if)# ip policy route-map PBR-VRF-SELECTION
Router(config-if)# ip vrf receive VRF_1
Router(config-if)# ip vrf receive VRF_2
Router(config-if)# end
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip vrf	Configures a VRF routing table.
ip vrf select source	Enables VRF selection on an interface.

Command	Description
set vrf	Enables VRF selection and filtering under a route map.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF selection table.

set vrf

To enable Virtual Private Network (VPN) routing/forwarding instance (VRF) selection within a route map for policy-based routing VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf *vrf-name*

no set vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to the VRF.

Command Default

No default behavior or values

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the MPLS VPN—VRF Selection using Policy Based Routing feature to provide a PBR mechanism for VRF selection. This command is used to enable VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. Match criteria is defined in an IP access list or in an IP prefix list. Match criteria can also be defined based on packet length with the **match length** route map command. The VRF must be defined prior to the configuration of this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be printed in the console when you attempt to configure the **set vrf** command.

Note The **set vrf** command cannot be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** policy routing commands because a packet cannot be set to an interface and the next hop cannot be changed when the VRF is specified. This is designed behavior. An error message will be printed in the console if you attempt to configure the **set vrf** command with any of the four above set clauses

Examples

The following example shows a route-map sequence that selects and sets a VRF based on match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
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
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.