MPLS VPN VRF Selection Using Policy-Based Routing

Last Updated: December 15, 2011

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.

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 Table at the end of this document.

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

Prerequisites for VRF Selection Using Policy-Based Routing

The router must support PBR.

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

The VRF Selection Using Policy-Based Routing feature 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 policy route-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 a match criterion for this feature.

The VRF Selection Using Policy-Based Routing feature cannot be configured with IP prefix lists.

Information About VRF Selection Using Policy-Based Routing

Introduction to 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 are defined in an IP access list or based on packet length. The following match criteria are supported in Cisco 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 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 Overview

When you are 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 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.

How to Configure VRF Selection Using Policy-Based Routing

Defining the Match Criteria for PBR VRF Selection Based on Packet Length

The match criteria for PBR VRF route selection are defined in an access list. Standard and named access lists are supported. Match criteria can also be defined based on the packet length using the **match length** route-map configuration command. This configuration option is defined entirely within a route map.

Prerequisites

Before you perform this task, make sure that the VRF and associated IP address are already defined.

Configuring PBR VRF Selection with a Standard Access List

Use the following commands to create a standard access list and define the PBR VRF route selection match criteria in it in order to permit or deny the transmission of VPN traffic data packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source-addr* [*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-addr* [*source-wildcard*] [**log**] **Example:** `Router(config)# access-list 40 permit 10.1.0.0/24 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 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 10.1.0.0/24 subnet.

Configuring PBR VRF Selection with a Named Access List

Use the following commands to define the PBR VRF route selection match criteria in a named access list in order to permit or deny the transmission of VPN traffic data packets.

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-addr source-wildcard destination-addr 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-addr source-wildcard destination-addr 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 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

Use the following commands to configure the VRF through which the outbound VPN packets will be policy routed in order to permit or deny the transmission of VPN traffic data packets.

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.

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. Do one of the following:

   - **match ip address** {*acl-number* [*acl-number ...* | *acl-name ...*] | *acl-name* [*acl-name ...* | *acl-number ...*]}
   -
   - **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.
Step 3	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** Router(config)# route-map map1 permit 10	Enters route map configuration mode. Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

	Command or Action	Purpose

Step 4	Do one of the following:
	
	• **match ip address** {*acl-number* [*acl-number ...* | *acl-name ...*] | *acl-name* [*acl-name ... | acl-number ...*]}
	
	•
	
	• **match length** *minimum-length maximum-length*
	
	Example:
	`Router(config-route-map)# match ip address 1`
	
	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 3 to 200 bytes in size.

Step 5	**set vrf** *vrf-name* **Example:** `Router(config-route-map)# set vrf map1`	Defines which VRF to route 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 map1.
Step 6	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and enters global configuration mode.

Configuring PBR on the Interface

Use the following commands to filter incoming VPN traffic data packets. Incoming packets are filtered through the match criteria that are defined in the route map.

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.

> ✎
>
> **Note**
>
> • 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 policy route-map** commands on the same interface.
>
> >

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 0/1/0	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 VRF1	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-if)# exit	Exits interface configuration mode and enters global configuration mode.

Configuring IP VRF Receive on the Interface

Use the following commands to insert the IP address of an interface as a connected route entry in a VRF routing table. This will prevent dropped packets.

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

Command or Action	Purpose
Step 2 **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3 **interface** *type number* [*name-tag*] **Example:** `Router(config)# interface FastEthernet 0/1/0`	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.
Step 5 **ip vrf receive** *vrf-name* **Example:** `Router(config-if)# ip vrf receive VRF1`	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 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 each of the following steps in this section in the order specified.

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

Example Defining PBR VRF Selection in Access List

In the following example, three standard access lists are created to define match criteria for three different subnets. Any packets received on the FastEthernet 0/1/0 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, VRF1 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 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 FastEthernet0/1/0
 ip address 10.1.0.0/24 255.255.255.252
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF1
 ip vrf receive VRF2
 ip vrf receive VRF3
```

Example Verifying VRF Selection Using Policy-Based Routing

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-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
```

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 VRF1
  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 VRF2
  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 VRF3
    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
FastEthernet0/1/0       PBR-VRF-Selection
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
MPLS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Multiprotocol Label Switching Command Reference*
Route-map configuration commands	*Cisco IOS IP Routing Protocols Command Reference*

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 software 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 standards has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VRF Selection Using Policy-Based Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1   ***Feature Information for VRF Selection Using Policy-Based Routing***

Feature Name	Releases	Feature Information
MPLS VPN: VRF Selection Using Policy-Based Routing	Cisco IOS XE Release 2.2	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.
		In Cisco IOS XE Release 2.2, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
		The following commands were introduced or modified: **ip vrf receive**, **set vrf**.

Glossary

PBR --policy-based routing.

VPN --Virtual Private Network.

VRF --virtual routing and forwarding.