Directing MPLS VPN Traffic Using Policy-Based Routing

Last Updated: December 15, 2011

This module explains how to configure policy-based routing (PBR) to classify and forward Multiprotocol Label Switching (MPLS) 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 Directing MPLS VPN Traffic Using Policy-Based Routing

- Multiprotocol BGP (MP-BGP), Multiprotocol Label Switching (MPLS), Cisco Express Forwarding (CEF), and MPLS VPNs must be enabled in your network.
- The router must be running Cisco IOS software that supports policy-based routing (PBR).

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

- A VRF must be defined prior to the configuration of this feature. An error message is displayed in the console if no VRF exists.

Restrictions for Directing MPLS VPN Traffic Using Policy-Based Routing

- VRF Select is supported only in Service Provider (-p-) images.
- This feature can coexist with features that use VRF selection based on the source IP address, 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. The console returns an error message 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** command cannot be configured with the following commands in the same route map sequence:
    - **set ip default interface**
    - **set interface**
    - **set ip default next-hop**
    - **set ip next-hop**

A packet cannot be set to an interface or to a next hop when the **set vrf** command is specified. This is designed behavior. An error message is displayed if you attempt to configure the **set vrf** command with any of the above four set clauses.

- The VRF Selection using Policy Based Routing feature cannot be configured with IP prefix lists.
- 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.
- PBR can be configured on an interface where a VRF is defined. However, the console displays the following warning messages 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
```

Information About Directing MPLS VPN Traffic Using Policy-Based Routing

- Directing MPLS VPN Traffic Using Policy-Based Routing Overview, page 2
- VRF Selection Introduces a New PBR Set Clause, page 3

Directing MPLS VPN Traffic Using Policy-Based Routing Overview

This feature allows you to route VPN traffic based on the following match criteria:

- IP Access Lists -- 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-- 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. IP access list match criteria 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.

VRF Selection Introduces a New PBR Set Clause

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

- **set ip default interface**
- **set ip 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.

This feature introduces the fifth set clause that can be used to change normal routing and forwarding behavior. You can use the **set vrf** command 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, because a packet cannot 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 Policy-Based Routing To Direct MPLS VPN Traffic

Defining the Match Criteria

The match criteria is defined in an access list. Standard and extended access lists are supported. The following sections show how to configure each type of access list:

Match criteria can also be defined based on the packet length by configuring the **match length** route-map configuration command. You use a route map to configure VRF selection based on packet length. See the Configuring the Route Map and Specifying VRFs, page 6 for more information.

Prerequisites

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

- Defining Match Criteria with a Standard Access List, page 4
- Defining Match Criteria with an Extended Access List, page 4

Defining Match Criteria with 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 40 192.168.1.0 0.0.0.255 permit`	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.

Defining Match Criteria with an 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*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. **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	**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.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-ext-nacl)# exit`	Exits named access list configuration mode, and enters global configuration mode.

Configuring the Route Map and Specifying VRFs

You define a route map then assign an access list to it. Then you specify a VRF for the traffic that matches the criteria in the route map. Use the **set vrf** command to specify the VRF through which the outbound VPN packets are routed.

Define the VRF before configuring the route map; otherwise the console displays an error.

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*]
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. Enters route map configuration mode.

Step 4	Do one of the following:
	• **match ip address***acl-number* [*acl-number...* | *acl-name...*] | *acl-name* [*acl-name...* | *acl-number*]
	Example:
	`Router(config-route-map)# match ip address 1`
	Example:
	`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 send VPN packets that are successfully matched. • 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.

Applying a Route Map to an Interface

You apply a route map to the incoming interface with the ip policy route-map global configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
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* **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.
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 can be configured so that the receiving packets can be received by the router after being set to a specific VRF.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and enters global configuration mode.

Configuring IP VRF Receive on the Interface

You must add the source IP address 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*
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* **Example:** `Router(config)# interface FastEthernet 0/1`	Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
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.
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 enters privileged EXEC mode.

Verifying the Configuration

To verify that the configuration is correct, 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 is defined in the access list. Both named and numbered access lists are supported.

	Command or Action	Purpose
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 Directing MPLS VPN Traffic Using Policy-Based Routing

- Configuring Policy-Based Routing with a Standard Access List Example, page 11
- Verifying Policy-Based Routing Example, page 11

Configuring Policy-Based Routing with a Standard Access List Example

In the following example, three standard access lists are created to define match criteria for three different subnets. A route map called PBR-VRF-Selection is assigned to interface Ethernet 0/1. If interface Ethernet 0/1 receives a packet whose source IP address is part of the 10.1.0.0/24 subnet, that packet is sent to VRF_1.

```
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 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

Related Documents

Related Topic	Document Title
Basic MPLS VPNs	Configuring MPLS Layer 3 VPNs

Related Topic	Document Title
MPLS VPN Carrier Supporting Carrier	• MPLS VPN Carrier Supporting Carrier Using LDP and an IGP • MPLS VPN Carrier Supporting Carrier with BGP
MPLS VPN InterAutonomous Systems	• MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels • MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

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 obtain lists of supported MIBs by platform and Cisco software release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

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

Feature Information for Directing MPLS VPN Traffic 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 Directing MPLS VPN Traffic Using Policy-Based Routing

Feature Name	Releases	Feature Configuration Information
MPLS VPN--VRF Selection using Policy-Based Routing	12.3(7)T 12.2(25)S	This feature allows you to classify and forward VPN traffic based on match criteria, such as IP access lists and packet length.

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