MPLS VPN VRF Selection Using Policy-Based Routing

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, page 1
• Prerequisites for MPLS VPN VRF Selection Using Policy-Based Routing, page 2
• Restrictions for MPLS VPN VRF Selection Using Policy-Based Routing, page 2
• Information About MPLS VPN VRF Selection Using Policy-Based Routing, page 2
• How to Configure MPLS VPN VRF Selection Using Policy-Based Routing, page 4
• Configuration Examples for MPLS VPN VRF Selection Using Policy-Based Routing, page 11
• Additional References, page 13
• Feature Information for MPLS VPN VRF Selection Using Policy-Based Routing, page 13

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 MPLS VPN VRF Selection Using Policy-Based Routing

- The device must support policy-based routing (PBR). For platforms that do not support PBR, use the “MPLS VPN VRF Selection Based on Source IP Address” feature.
- A virtual routing and forwarding (VRF) instance must be defined prior to the configuration of this feature. An error message is displayed on the console if no VRF exists.
- Before you configure the MPLS VPN VRF Selection Using Policy-Based Routing feature, make sure that the VRF and associated IP address are already defined.
- This document assumes that multiprotocol Border Gateway Protocol (mBGP), Multiprotocol Label Switching (MPLS), and Cisco Express Forwarding are enabled in your network.

Restrictions for MPLS VPN VRF Selection Using Policy-Based Routing

- The MPLS VPN VRF Selection Using Policy-Based Routing feature is supported only in service provider (-p-) images.
- The MPLS VPN VRF Selection Using Policy-Based Routing feature can coexist with the MPLS VPN VRF Selection Based on Source IP address feature on the same device, but these features cannot be configured together on the same interface. This is designed behavior to prevent virtual routing and forwarding (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 policy-based routing (PBR) and cannot be configured for a source IP address that is a match criterion for this feature.
- The MPLS VPN VRF Selection Using Policy-Based Routing feature cannot be configured with IP prefix lists.

Information About MPLS VPN VRF Selection Using Policy-Based Routing

Introduction to MPLS VPN VRF Selection Using Policy-Based Routing

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. The policy-based routing (PBR) implementation of the virtual routing and forwarding (VRF) selection feature allows you to policy route Virtual Private Network (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 policy-based routing (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 MPLS VPN 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 virtual routing and forwarding (VRF) instance after the successful match occurs in the route map.

Match Criteria for Policy-Based Routing VRF Selection Based on Packet Length

The match criteria for policy-based routing (PBR) virtual routing and forwarding (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.
How to Configure MPLS VPN VRF Selection Using Policy-Based Routing

Configuring Policy-Based Routing VRF Selection with a Standard Access List

Use the following commands to create a standard access list and define the policy-based routing (PBR) virtual routing and forwarding (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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`access-list access-list-number {deny</td>
<td>permit} source-addr [source-wildcard] [log]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# access-list 40 permit 10.1.0.0/24 0.0.0.255</code></td>
<td>• 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.</td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>
configuring policy-based routing vrf selection with a named access list

use the following commands to define the policy-based routing (pbr) virtual routing and forwarding (vrf) route selection match criteria in a named access list in order to permit or deny the transmission of virtual private network (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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip access-list {standard</td>
<td>extended} [access-list-name</td>
</tr>
<tr>
<td>Example: Device(config)# ip access-list extended NAMEDACL</td>
<td>- A standard, extended, or named access list can be used.</td>
</tr>
<tr>
<td><strong>Step 4</strong> [sequence-number] {permit</td>
<td>deny} protocol source-addr source-wildcard destination-addr destination-wildcard [option option-value] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</td>
</tr>
<tr>
<td>Example: Device(config-ext-nacl)# permit ip any any option any-options</td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- The example creates a named access list that permits any configured IP option.</td>
</tr>
</tbody>
</table>
Configuring Policy-Based Routing VRF Selection in a Route Map

Use the following commands to configure the VRF through which the outbound Virtual Private Network (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.

**Before You Begin**

- The virtual routing and forwarding (VRF) instance 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`route-map map-tag [permit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>- `match ip address {acl-number [acl-number ...</td>
</tr>
<tr>
<td></td>
<td>- <code>match length minimum-length maximum-length</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>set vrf vrf-name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Policy-Based Routing on the Interface

Use the following commands to filter incoming Virtual Private Network (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 MPLS VPN VRF Selection Using Policy-Based Routing feature can coexist with the MPLS VPN VRF Selection Based on Source IP address feature on the same device, but the two features cannot be configured together on the same interface. This is designed behavior to prevent virtual routing and forwarding (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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type number [name-tag]</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface FastEthernet 0/1/0</td>
<td></td>
</tr>
</tbody>
</table>
### 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 virtual routing and forwarding (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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Purpose

**Command or Action**

- `ip policy route-map map-tag`

**Purpose**

Identifies a route map to use for policy routing on an interface.

- The configuration example attaches the route map named `map1` to the interface.

**Example:**

```
Device(config-if)# ip policy route-map map1
```

### Step 5

**Command or Action**

- `ip vrf receive vrf-name`

**Purpose**

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.

**Example:**

```
Device(config-if)# ip vrf receive VRF1
```

### Step 6

**Command or Action**

- `exit`

**Purpose**

Exits interface configuration mode and enters global configuration mode.

**Example:**

```
Device(config-if)# exit
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Step 2**

configure terminal

**Example:**
Device# configure terminal

**Step 3**

interface type number [name-tag]

**Example:**
Device(config)# interface FastEthernet 0/1/0

**Step 4**

ip policy route-map map-tag

**Example:**
Device(config-if)# ip policy route-map map1

• The configuration example attaches the route map named map1 to the interface.

**Step 5**

ip vrf receive vrf-name

**Example:**
Device(config-if)# ip vrf receive VRF1

• This command must be configured for each VRF that will be used for VRF selection.

**Step 6**

end

**Example:**
Device(config-if)# end

---

### Verifying the Configuration of the MPLS VPN VRF Selection Using Policy-Based Routing

**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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>show ip access-list [access-list-number</td>
<td>access-list-name]</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show ip access-list</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>show route-map [map-name]</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show route-map</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip policy</td>
<td>Displays the route map used for policy routing.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show ip policy</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Examples for MPLS VPN VRF Selection Using Policy-Based Routing**

**Example: Defining Policy-Based Routing VRF Selection in an 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 policy-based routing (PBR) VRF selection route map to the virtual routing and forwarding (VRF) instancer 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.

```plaintext
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
```
Examples: Verifying VRF Selection Using Policy-Based Routing

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

Example: Verifying Match Criteria

To verify the configuration of match criteria for policy-based routing (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:

```
Device# 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
```

Example: 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.

```
Device# show route-map
route-map PBR-VRF-Selection, permit, sequence 10
  Match clauses:
    ip address {access-lists}: 40
    vrf VRF1
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 20
  Match clauses:
    ip address {access-lists}: 50
    vrf VRF2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 30
  Match clauses:
    ip address {access-lists}: 60
    vrf VRF3
  Policy routing matches: 0 packets, 0 bytes
```
Example: Verifying Policy-Based Routing VRF Selection Policy

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

```
Device# show ip policy
Interface   Route map
FastEthernet0/1/0 PBR-VRF-Selection
```

Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco Master Command List, All Releases</td>
</tr>
<tr>
<td>MPLS and MPLS applications commands</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for MPLS VPN 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 MPLS VPN VRF Selection Using Policy-Based Routing

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS VPN VRF Selection Using Policy-Based Routing</td>
<td>12.3(7)T, 12.2(25)S, 12.2(33)SRB, 12.2(33)SXI, Cisco IOS XE Release 2.2</td>
<td>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 Release 12.3(7)T, this feature was introduced. In Cisco IOS Releases 12.2(25)S, 12.2(33)SRB, and 12.2(33)SXI, this feature was integrated. In Cisco IOS XE Release 2.2, this feature was implemented on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: ip vrf receive, set vrf.</td>
</tr>
</tbody>
</table>