MPLS VPN: VRF Selection Based on Source IP Address

The VPN Routing and Forwarding (VRF) Selection feature allows a specified interface on a provider edge (PE) router to route packets to different Virtual Private Networks (VPNs) based on the source IP address of the packet. This feature is an improvement over using a policy-based router to route packets to different VPNs.

History for the MPLS VPN: VRF Selection Based on Source IP Address Feature

Release	Modification
12.0(22)S	This feature was introduced on the Cisco 12000 Series Internet Router
12.0(23)S	This feature was updated to support the following line cards: • 1-port 10-Gigabit Ethernet (E4+) • 3-port Gigabit Ethernet • Modular Gigabit Ethernet (E4+)
12.0(24)S	Support for the Cisco 12000 Series Internet Router engine 3 was added.
12.2(14)SZ	This feature was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This feature was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This feature was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	Support was added for the PRE3 on the Cisco 10000 Series Router.

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

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- Prerequisites for MPLS VPN: VRF Selection Based on Source IP Address, page 2
- Restrictions for MPLS VPN: VRF Selection Based on Source IP Address, page 3
- Information About MPLS VPN: VRF Selection Based on Source IP Address, page 3
- How to Configure VRF Selection Based on Source IP Address, page 8
- Configuration Examples for VRF Selection Based on Source IP Address, page 12
- Additional References, page 14
- Command Reference, page 15

Prerequisites for MPLS VPN: VRF Selection Based on Source IP Address

- MPLS VPNs must be enabled in the provider network.
- For the Cisco 12000 Internet Router Series must contain one of the following line cards:

  Engine 0:

  - 1-port OC-12 POS
  - 4-port OC-3 POS
  - 6- and 12- port DS3

  Engine 2:

  - 1-port OC-48 POS
  - 4-port OC-12 POS
  - 8- and 16-port OC-3 POS
  - 3-port Gigabit Ethernet

  Engine 3:

  - 4-port OC-12c/STM-4c POS ISE
  - 4-port CHOC-12 ISE
  - 1-port OC-48c POS ISE
  - 1-port CHOC-48 ISE
  - 4-, 8-, and 16-port OC-3c POS ISE

  Engine 4:

  - 4-port OC-48 POS

- OC-192 E4+ POS
- 1-port 10-Gigabit Ethernet (E4+)
- Modular Gigabit Ethernet (E4+)

Restrictions for MPLS VPN: VRF Selection Based on Source IP Address

- VRF Select is supported only in Service Provider (-p-) images.
- The Cisco IOS software must support MPLS VPNs, and the provider network must have MPLS Label Distribution Protocol (LDP) installed and running.
- The VRF Selection feature is a unidirectional feature and can only be used from a customer (IP-based) network for a connection to a provider (MPLS-based) network and cannot be used from a provider network to a customer network.
- Subnet masks should be kept as short as possible for the VRF Selection criteria for Engine 2 line cards. VRF Selection performance can degrade with longer subnet masks (/24 or /32, for example).
- Cisco Express Forwarding (CEF) must be enabled on any interfaces that have the VRF Selection feature enabled. Distributed CEF is enabled by default on Cisco 12000 Series Internet routers.
- An IP traceroute command from an MPLS VPN VRF Selection CE router to a typical MPLS VPN VRF CE router works as expected. However, an IP traceroute command from a typical MPLS VPN VRF CE router to an MPLS VPN VRF Selection CE router might fail to show all the relevant hop information across the core.

Information About MPLS VPN: VRF Selection Based on Source IP Address

The VRF Selection feature allows packets arriving on an interface to be switched into the appropriate VRF table based upon the source IP address of the packets. Once the packets have been “selected” into the correct VRF routing table, they are processed normally, based on the destination address and forwarded through the rest of the Multiprotocol Label Switching (MPLS) VPN.

In most cases, the VRF Selection feature is a “one way” feature; it works on packets coming from the end users to the PE router.

VRF Selection Process

The VRF Selection feature uses the process described in this section to route packets from the customer networks to the PE router and into the provider network.

A two-table lookup mechanism is used at the ingress interface of the PE router to determine the routing and forwarding of packets coming from the customer networks, which use IP protocols, to the MPLS VPN networks, which use MPLS protocols.

- The first table, the VRF Selection table, is used to compare the source IP address of the packet with a list of IP addresses in the table. Each IP address in the table is associated with an MPLS VPN. If a match is found between the source IP address of the packet and an IP address in the VRF Selection table, the packet is routed to the second table (the VRF table) or the routing table for the appropriate VPN.

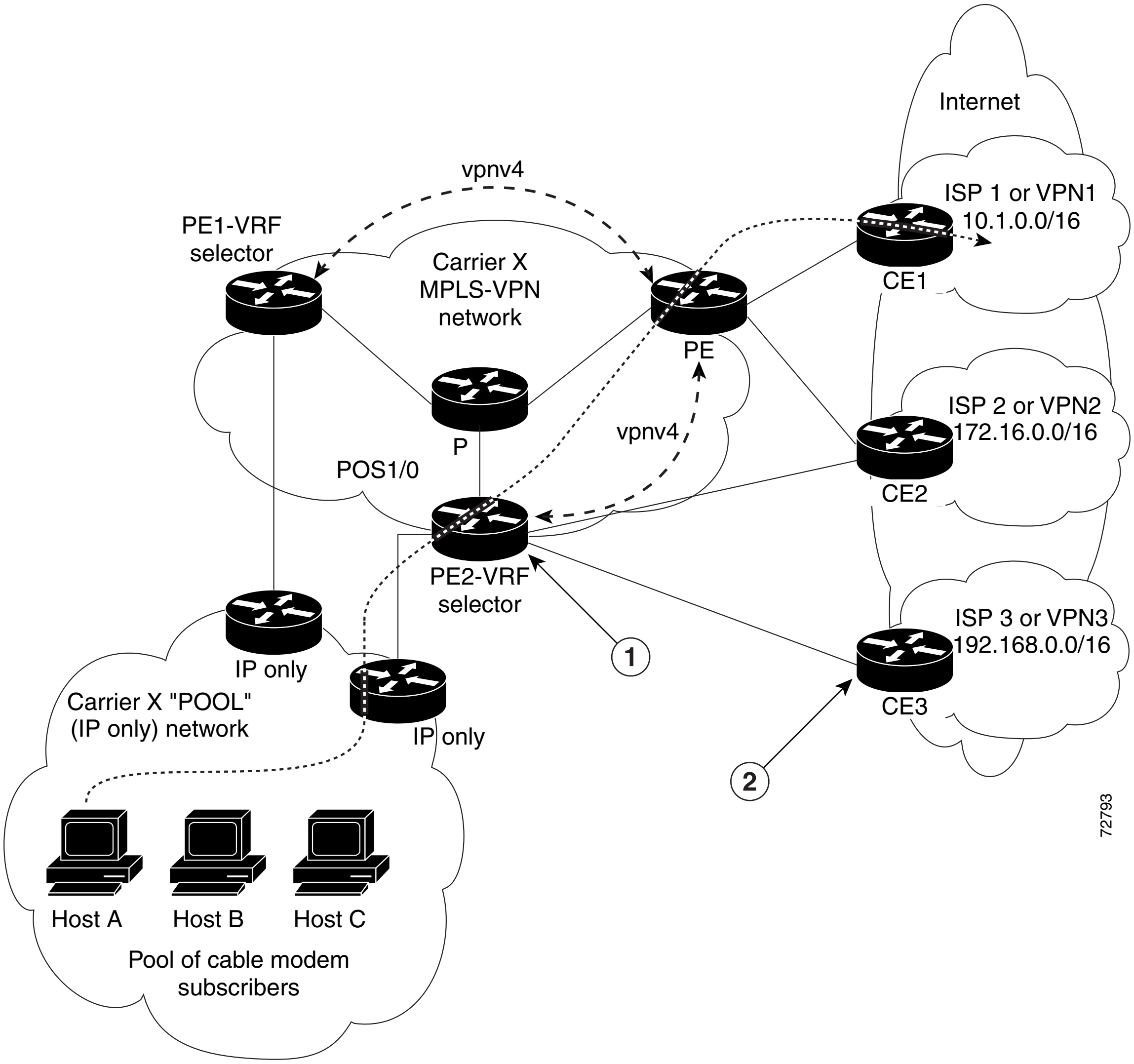
  If no match is found in the table for the source IP address of the packet, the packet is either routed via the global routing table used by the PE router (this is the default behavior), or is dropped. See the "Configuring a VRF to Eliminate Unnecessary Packet Forwarding: Example" section on page 14 for more information.
- The second table, the VRF table (also known as the VPN routing table), contains the virtual routing and forwarding information for the specified VPN and is used to forward the selected VPN traffic to the correct MPLS label switched path (LSP) based upon the destination IP address of the packet.

The VRF Selection process removes the association between the VPN and the interface and allows more than one MPLS VPN to be associated with the interface.

VRF Selection Examples

Here is an example of the VRF Selection feature. It is based on a network carrier that allows subscribers to the carrier to choose from multiple Internet service providers (ISPs) for Internet access. Figure 1 provides an example of the VRF Selection feature with an IP-based host network, an MPLS VPN network, and three ISPs connected to the MPLS VPN network.

Figure 1 VRF Selection Implementation Example



1	PE2 is acting as a VRF selector and as a typical MPLS VPN PE router to CE2 and CE3.	**2**	ISPs 1 to 3 provide a list of IP addresses to Carrier X so that each host in the “POOL” network can be properly addressed. This host addressing would most likely be done by means of the DHCP or DNS services of Carrier X.

In Figure 1, Carrier X represents the network carrier; Host A, Host B and Host C represent the carrier subscribers; and ISP 1, ISP 2 and ISP 3 represent the ISPs.

Figure 1 illustrates a packet traveling from Host A to ISP 1. The dashed line represents the travel of the packet.

Host A chooses ISP 1 to use as its ISP. Carrier X will provide an IP address to Host A that falls within the range of the ISP 1 registered network addresses. Based upon this IP address allocation, the VRF Selection criteria are set.

The POOL network, by using default routes, forwards traffic from the Carrier X IP-based (POOL) network to the Carrier X MPLS-based VPN network. The MPLS VPN network forwards (shunts) the traffic from Host A into the correct VPN, which is VPN 1 (ISP 1), by using the VRF Selection-enabled router PE2.

To enable the VRF Selection feature on the routers PE1 and PE2, enter the following commands:

```
Router(config)# vrf selection source 10.1.0.0 255.255.0.0 vrf vpn1
Router(config)# vrf selection source 172.16.0.0 255.255.0.0 vrf vpn2
Router(config)# interface POS1/0
Router(config-if)# description Link to CE POS1/0
Router(config-if)# ip vrf select source
```

For more information on the commands used to configure the VRF Selection feature, see the "Command Reference" section on page 15.

The VRF Selection feature is a one-way (unidirectional) feature in most implementations; it only works on packets coming from the customer networks to a PE router. See the "VRF Selection is a Unidirectional Feature" section on page 6 for more information.

Traffic coming from the ISPs to the hosts (in the example, traffic traveling from the ISPs on the right to the hosts on the left) is not affected by the VRF Selection feature and does not have to be returned via an MPLS path. This traffic can return via the shortest available IP path.

Another example of VRF Selection in use might involve a cable modem termination system (CMTS). If the owner of the CMTS wants to allow cable modem subscribers to choose their ISP from a group of ISPs, the VRF Selection feature provides a fast and scalable solution.

VRF Selection is a Unidirectional Feature

In Figure 1, the end users are typical Internet home users. If the VRF Selection feature were a two-way (bidirectional) feature, traffic coming from the ISPs to the hosts would be required to use only the PE routers that have VRF Selection enabled, which might cause performance issues.

When traffic from the POOL network goes through the carrier network to the ISP networks for Internet access, the traffic in the carrier network must be forwarded by means of MPLS VPN paths, because the VRF Selection-enabled router has "selected" the traffic into the correct MPLS VPN.

Traffic from the ISP networks to the POOL network does not have to use MPLS VPN paths in the carrier network and can use the path that seems most efficient to return to the POOL network. This traffic can use a path that uses either MPLS or IP for routing and forwarding and does not have to travel via an MPLS VPN.

Traffic from the ISP networks to the POOL networks can be forwarded by the global routing table used by every interface. One way to accomplish this is to enter VRF static routes on the PE router interfaces connected to the ISPs. The VRF static routes would route traffic from the ISPs to the carrier network. See "Establishing IP Static Routes for a VRF Instance" section on page 10 for information on placing a default VRF static route onto an interface.

Establishing static VRF routes allows traffic from the ISPs to enter the carrier network as traffic that can only be routed by using the global routing table toward the POOL network.

If the ISPs are not providing global host address space, or the VRF feature is not being used to route Internet traffic, the PE interfaces connected to the ISPs must be placed into a VRF. If the PE interfaces are using VRFs for routing traffic from the ISPs, all traffic from the ISPs to the hosts through the carrier network would be forwarded by MPLS VPN paths, and performance would not be as good as if IP forwarding were used.

Normal IP-based VPN operations, such as populating the routing information base (RIB) and forwarding information base (FIB) from a routing protocol such as Border Gateway Protocol (BGP), are used to route and forward packets within the various VPNs in the customer networks. The provider network uses MPLS-based routing protocols to perform VPN routing and forwarding inside the provider network.

See the "Configuring VRF Selection" section on page 9 for a sample configuration of the VRF Selection feature.

Conditions Under Which VRF Selection Becomes Bidirectional

Forwarding of traffic from the carrier network to the POOL network by using the global routing table is possible only if the ISPs have provided registered IP address space for all of the subscribed users within the POOL network.

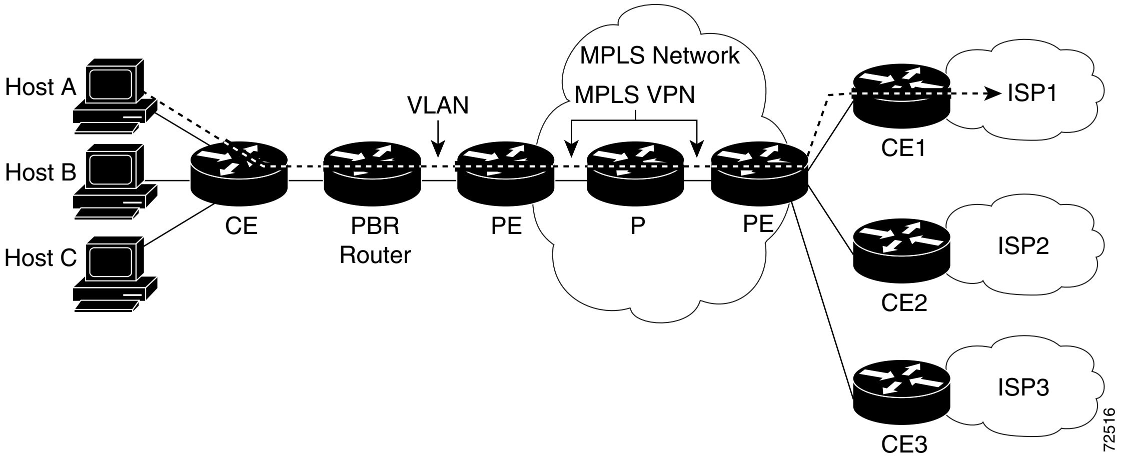
If the POOL network uses IP addresses that are not globally routeable and are designed for a nonconnected enterprise (defined by RFC1918), the VRF Selection feature becomes bidirectional. All traffic being sent and received by the host would have to travel via a router that has the VRF Selection feature enabled. The POOL network cannot be addressed with overlapping address space, regardless of the type of address space being used.

Advantages of VRF Selection over Per-Interface IP VPN Configuration

The VRF Selection feature removes the association between a VPN and an interface. Before the VRF Selection feature was introduced, the following implementation was used to route outgoing MPLS VPN packets to different destinations:

- A policy-based router (PBR) is attached to the customer edge (CE) router.
- The egress side of the PBR router side has VLANs connected to a PE.
- The PBR router uses a policy-based route map to select the correct output (VLAN) interface, and each VLAN is under a specific VRF. Figure 2 illustrates a sample configuration in which a PBR router is used for routing MPLS packets to different destinations.

Figure 2 Implementation of Multiple VPNs Before VRF Selection



The following limitations apply to PBR-based solutions that use this implementation:

- Policy routing and MPLS VPN functions cannot be performed on the same platform. Integration into a single platform is critical for manageability and support.
- Each VRF is limited to one VPN per interface, which limits scalability.
- There is no network redundancy.
- The PBR is the only point of connection for all the networks attached to the PBR. The capacity and the performance capabilities of the PBR router are critical.
- There is no diversity in the connectivity to the networks.
- Every network is required to connect to every PBR. If every network is not connected to every PBR, packets from the end user to the PBR are dropped because the PBR has no way of switching the IP traffic properly.
- Adding multiple PBRs that are interconnected introduces more network policy-routed hops.

The VRF Selection feature addresses the limitations of and problems with using a PBR for packet routing and forwarding.

Benefits of VRF Selection Based on Source IP Address

The following are benefits to using the VRF Selection method of VPN routing and forwarding.

- **Association of VPN to interface is removed**–The VRF Selection feature removes the association between a VPN and an interface, thus allowing packets from the host network to the provider network to have more than one VPN available per interface.
- **Access to every customer network is possible from every PE router in the provider network**–Access points to each network can be established at any MPLS PE router and can be made redundant by connections to multiple PE routers (for example, the CE2 router in Figure 1 on page 5).
- **Multiple points in the provider network can be used for VPN routing and forwarding**–MPLS VPNs, like IP, are connectionless. Any PE router, whether VRF Selection-enabled or not, is capable of carrying VRF Selection traffic from the MPLS network out to the CE routers.

How to Configure VRF Selection Based on Source IP Address

This section contains the following procedures:

- Configuring VRF Selection (required)
- Establishing IP Static Routes for a VRF Instance (optional)
- Verifying VRF Selection (optional)

Configuring VRF Selection

To add a source IP address to a VRF Selection table, use the following commands, beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf selection source** *source-IP-address source-IP-mask* **vrf** *vrf_name*
4. **ip vrf select source**
5. **ip vrf receive** *vrf_name*

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	**vrf selection source** *source-IP-address source-IP-mask* **vrf** *vrf_name* **Example:** `Router(config)# vrf selection source 172.16.0.0 255.255.0.0 vrf test`	Populates a single source IP address, or range of source IP addresses, to a VRF Selection table.
Step 4	**ip vrf select source** **Example:** `Router(config-if)# ip vrf select source`	Enables the VRF Selection feature on an interface.
Step 5	**ip vrf receive** *vrf_name* **Example:** `Router(config-if)# ip vrf receive red`	Adds all the IP addresses that are associated with an interface into a VRF table.

Establishing IP Static Routes for a VRF Instance

Traffic coming from the ISPs to the hosts does not require the use of the MPLS VPN paths; this traffic can use the shortest IP route back to the host.

VPN static routes for traffic returning to the customer networks are only necessary if VPN traffic returning to the customer networks is being forwarded from the VRF Selection interface. The remote PE router could also be configured to route return traffic to the customer networks directly by using the global routing table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *vrf vrf_name prefix mask* [*next-hop-address*] [**interface** {*interface-number*}] [**global**] [**distance**] [**permanent**] [**tag** *tag*]

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	**`ip route`** *`vrf vrf_name prefix mask`* [*`next-hop-address`*] [`interface` {*`interface-number`*}] [`global`] [`distance`] [`permanent`] [`tag` *`tag`*] **Example:** `Router(config-if)# ip route vrf vpn1 172.16.0.0 255.255.0.0 POS1/0`	Establishes static routes for a VRF.

Verifying VRF Selection

Enter the **show ip route vrf** command in EXEC mode to display the IP routing table associated with a VRF instance. This example shows the IP routing table associated with the VRF vrf1:

```
Router# show ip route vrf vpn1
Routing Table: vpn1
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
Gateway of last resort is not set
B    10.0.0.0/8 [200/0] via 10.10.10.10, 00:00:37
     172.16.0.0/16 is subnetted, 1 subnets
B       10.19.0.0 [200/0] via 10.10.10.10, 00:00:37
     10.0.0.0/32 is subnetted, 1 subnets
B       10.14.14.14 [200/0] via 10.10.10.10, 00:00:37
     10.0.0.0/32 is subnetted, 1 subnets
S       10.15.15.15 [1/0] via 10.0.0.1, POS1/1
```

Troubleshooting Tips

- Enter the **debug vrf select** command to enable debugging for the VRF Selection feature.

Note The **debug vrf select** command can cause many messages to be logged when you change the configuration and when switching occurs.

- The following error messages appear if problems occur while configuring the VRF Selection feature:
  - If you attempt to configure a nonexisting VRF Selection table:

    ```
    Router(config)#vrf selection source 172.16.0.0 255.255.0.0 vrf VRF_NOEXIST
    VRF Selection: VRF table VRF_NOEXIST does not exist.
    ```

  - If you attempt to remove a VRF Selection entry that does not exist:

    ```
    Router(config)#no vrf selection source 172.16.0.0 255.255.0.0 vrf VRF1
    VRF Selection: Can't find the node to remove.
    ```

  - If you attempt to configure a duplicate IP address and subnet mask for a VRF Selection entry:

    ```
    Router(config)#vrf selection source 172.16.0.0 255.0.0.0 vrf VRF_AOL
    Router(config)#vrf selection source 172.16.0.0 255.0.0.0 vrf VRF_AOL
    VRF Selection: duplicate address and mask configured.
    ```

  - If an inconsistent IP address and mask are used for a VRF Selection entry:

    ```
    Router(config)#vrf selection source 172.16.2.1 255.255.255.0 vrf red
    % Inconsistent address and mask
    Router(config)#vrf selection source 172.16.2.1 255.255.255.255 vrf red
    ```

  - If you attempt to configure a VRF instance on an interface that has VRF Selection already configured:

    ```
    Router(config-if)#ip vrf select source
    Router(config-if)#ip vrf forward red
    % Can not configure VRF if VRF Select is already configured
    ```

```
To enable VRF, first remove VRF Select from the interface
```

- If you attempt to configure a VRF Selection entry on an interface that has VRF already configured:

```
Router(config-if)#ip vrf forward red
Router(config-if)#ip vrf select source
% Can not configure VRF Select if interface is under a non-global VRF
To enable VRF Select, first remove VRF from the interface
```

Configuration Examples for VRF Selection Based on Source IP Address

- Enabling MPLS VPNs: Example
- Creating a VRF Routing Table: Example
- Defining VRF Selection Entries: Example
- Defining IP Static Routes for a VRF: Example
- Configuring an Interface for VRF Selection: Example
- Configuring a BGP Router for VRF Selection: Example
- Configuring a VRF to Eliminate Unnecessary Packet Forwarding: Example
- Command Reference

Enabling MPLS VPNs: Example

The following example shows how to enable the router to accept MPLS VPNs:

```
Router(config)# mpls label protocol ldp
Router(config)# interface loopback0
Router(config-if)# ip address 10.13.13.13 255.255.255.255
Router(config-if)# no ip directed-broadcast
```

Creating a VRF Routing Table: Example

The following example shows how to create two VRF Selection tables (vpn1 and vpn2):

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 1000:1
Router(config-vrf)# route-target export 1000:1
Router(config-vrf)# route-target import 1000:1
Router(config-vrf)# exit
Router(config)# ip vrf vpn2
Router(config-vrf)# rd 1000:2
Router(config-vrf)# route-target export 1000:2
Router(config-vrf)# route-target export 1000:2
```

Defining VRF Selection Entries: Example

The following example shows two entries (vpn1 and vpn2) being defined in the VRF Selection table. In this example, packets with the source address of 10.16.0.0 will be routed to the VRF vpn1, and packets with the source address of 10.17.0.0 will be routed to the VRF vpn2:

```
Router(config)# vrf selection source 10.16.0.0 255.255.0.0 vrf vpn1
Router(config)# vrf selection source 10.17.0.0 255.255.0.0 vrf vpn2
```

Defining IP Static Routes for a VRF: Example

The following example shows IP static routes being created for two VRFs (vpn1 and vpn2) for the POS1/0 interface:

```
Router(config)# ip route vrf vpn1 10.16.0.0 255.255.0.0 POS1/0
Router(config)# ip route vrf vpn2 10.17.0.0 255.255.0.0 POS1/0
```

Configuring an Interface for VRF Selection: Example

The following example shows the POS1/0 interface being configured for the VRF Selection feature and the configured IP address (31.0.0.1) being added to the VRFs vpn1 and vpn2 as connected routes:

```
Router(config)# interface POS1/0
Router(config-if)# description Link to CE1 POS1/0 (eng2)
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive vpn1
Router(config-if)# ip vrf receive vpn2
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# load-interval 30
Router(config-if)# crc 32
Router(config-if)# end
```

Configuring a BGP Router for VRF Selection: Example

A router that is VRF Selection-enabled requires an MPLS VPN BGP configuration. The following example configures a router that is using BGP for the VRF Selection feature:

```
Router(config)# router bgp 1000
Router(config-router)# no bgp default ipv4-unicast
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# timers bgp 10 30
Router(config-router)# neighbor 10.11.11.11 remote-as 1000
Router(config-router)# neighbor 10.11.11.11 update-source Loopback0
Router(config-router)# no auto-summary

Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.11.11.11 activate
Router(config-router-af)# neighbor 10.11.11.11 send-community extended
Router(config-router-af)# exit-address-family

Router(config-router)# address-family ipv4 vrf vpn2
Router(config-router-af)# redistribute static
Router(config-router-af)# no auto-summary
Router(config-router-af)# no synchronization
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf vpn1
Router(config-router-af)# redistribute static
Router(config-router-af)# no auto-summary
Router(config-router-af)# no synchronization
Router(config-router-af)# exit-address-family
```

Configuring a VRF to Eliminate Unnecessary Packet Forwarding: Example

If a packet arrives at an interface that has VRF Selection enabled, and the packet source IP address does not match any VRF Selection definition, that packet will be forwarded by means of the global routing table. This default behavior could cause problems if IP address spoofing is being implemented. Unnecessary traffic could be forwarded by the global routing table. To eliminate this unnecessary routing of packets, create a VRF Selection definition that will forward all unknown incoming traffic to a null interface.

The following configuration causes all traffic not matching a more specific VRF Selection definition to be routed to the Null0 interface, thus causing the packets to be dropped.

```
Router(config)# ip vrf VRF_DROP
Router(config-vrf)# rd 999:99
Router(config-vrf)# route-target export 999:99
Router(config-vrf)# route-target import 999:99
Router(config-vrf)# exit

Router(config)# vrf selection source 0.0.0.0 0.0.0.0 vrf VRF_DROP

Router(config)# ip route vrf VRF_DROP 0.0.0.0 0.0.0.0 Null0
```

Additional References

The following sections provide references related to **MPLS VPN: VRF Selection Based on Source IP AddressFeature**.

Related Documents

Related Topic	Document Title
MPLS VPNs	*MPLS Virtual Private Networks*

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	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
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new commands only.

- **ip vrf receive**
- **ip vrf select source**
- **vrf selection source**

ip vrf receive

To insert the IP address of an interface as a connected route entry in a Virtual Private Network (VPN) routing/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.

Defaults

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.

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 (CEF) 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 CEF 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 172.16.1.3 255.255.255.252
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 192.168.1.2 255.255.255.252
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.
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.

ip vrf select source

To enable the VRF Selection feature on a particular interface or subinterface, use the **ip vrf select source** command in interface configuration mode. To disable the VRF Selection feature on a particular interface or subinterface, use the **no** form of this command.

ip vrf select source

no ip vrf select source

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The **ip vrf select source** and **ip vrf forwarding** commands are mutually exclusive. If the VRF Selection feature is configured on an interface, you cannot configure VRFs (using the **ip vrf forwarding** command) on the same interface.

Examples

The following example shows how to enable the VRF Selection feature on an interface:

```
Router(config-if)# ip vrf select source
```

The following example shows the message you receive after you have deleted the VRF Selection feature on an interface:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# int pos4/0
Router (config-if)# no ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT unset for POS4/0, slot: 4
Router (config-if)#
```

The following example shows the message you receive after you have enabled the VRF Selection feature on an interface:

```
Router (config-if)#
Router (config-if)# ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT set for POS4/0, slot: 4
Router (config-if)#
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF Selection table.

vrf selection source

To populate a single source IP address, or range of source IP addresses, to a VRF Selection table, use the **vrf selection source** command in global configuration mode. To remove a single source IP address or range of source IP addresses from a VRF Selection table, use the **no** form of this command.

vrf selection source *source-IP-address source-IP-mask* **vrf** *vrf_name*

no vrf selection source *source-IP-address source-IP-mask* **vrf** *vrf_name*

Syntax Description

source-IP-address	New source IP address to be added to the VRF Selection table.
source-IP-mask	IP mask for the source IP address or range of single source IP addresses to be added to the VRF Selection table.
vrf *vrf_name*	Name of the VRF Selection table to which the single source IP address or range of source IP addresses should be added.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

If a VRF table is removed by using the **no ip vrf** *vrf_name* command in global configuration mode, all configurations associated with that VRF will be removed including those configurations added with the **vrf selection source** command.

Examples

The following example shows how to populate the VRF Selection table vpn1 with a source IP network address 10.0.0.0 and the IP mask 255.0.0.0, which would forward any packets with the source IP address 10.0.0.0 into the VRF instance vpn1:

```
Router(config)# vrf selection source 10.0.0.0 255.0.0.0 vrf vpn1
```

The following example shows the message you receive after you have removed the source IP network address 107.1.1.1 and the IP mask 255.255.255.255 from the VRF Selection table vpn1:

```
Router (config)# no vrf selection source 10.1.1.1 255.255.255.255 vrf vpn1
Router (config)#
VRF Selection Configuration: addr:10.1.1.1, mask:255.255.255.255, vrf_name:vpn1

5d13h: VRF Selection Remove Configuration: addr:10.1.1.1, mask: 255.255.255.255
Router (config)#
```

The following example shows the message you receive after you have added the source IP network address 10.1.1.1 and the IP mask 255.255.255.255 to the VRF Selection table vpn1:

```
Router (config)# vrf selection source 10.1.1.1 255.255.255.255 vrf vpn1
Router (config)#
VRF Selection Configuration: addr:10.1.1.1, mask:255.255.255.255, vrf_name:vpn1
VRF Selection: VRF table vpn1, id is: 1
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
ip vrf select source	Enables VRF Selection on an interface.