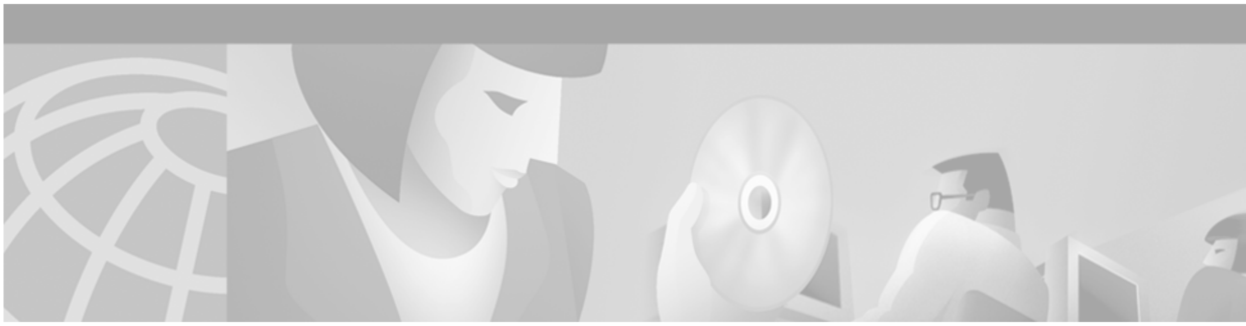


MPLS VPN—VRF Selection Based on Source IP Address

Feature History

Release	Modification
12.0(22) S	This feature was introduced.

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.

This document includes the following sections:

Feature Overview

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 upon 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 following process 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.

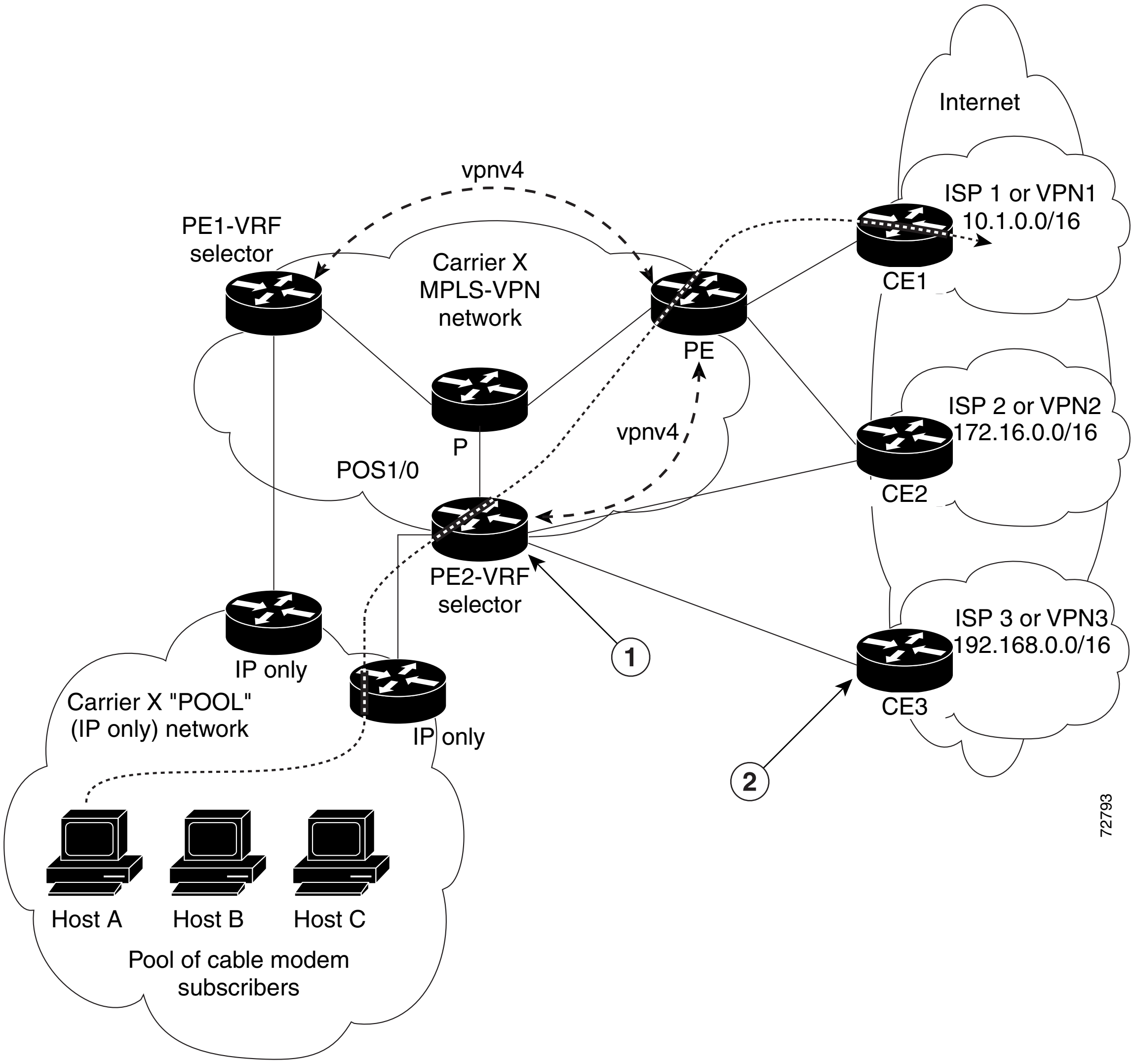
  If no match is found in the table for the source IP address of the packet, the packet will either be routed via the global routing table used by the PE router (this is the default behavior), or will be dropped. See the "Configuring a VRF to Eliminate Unnecessary Packet Forwarding" section on page 13 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

An example of the VRF Selection feature would be 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 both as a VRF selector and 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 using 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 (1.1.0.0/16). Based upon this IP address allocation, the VRF Selection criteria is 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 1.1.0.0 255.255.0.0 vrf vpn1
Router(config)# vrf selection source 2.2.0.0 255.255.0.0 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 14.

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 4 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 would be 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 was 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 using 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 any path that is 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 using 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 9 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 using MPLS VPN paths, and performance would not be as optimal as if IP forwarding was 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 only possible if the ISPs have provided registered IP address space for all of the subscribed users within the POOL network from the global routing table.

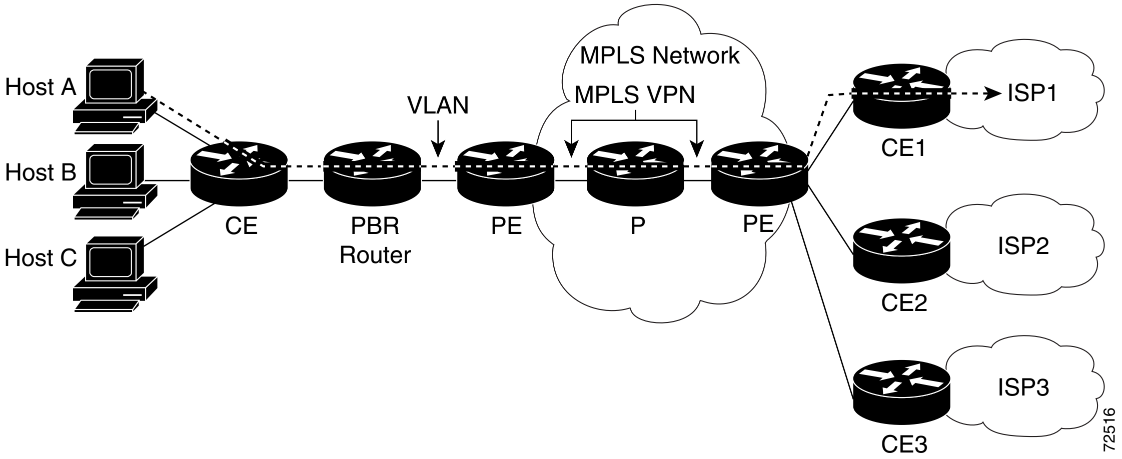
If the POOL network uses IP addresses that are not globally routeable and are designed for a non-connected enterprise (defined by RFC1918), the VRF Selection feature becomes bidirectional. All traffic being sent and received by the host would have to travel via a router that has the VRF Selection feature 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 of using a PBR router 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.
- VRF is limited to one VPN per interface, which limits scalability.
- The Cisco 7500 Series router is used for the PBR, which can limit network performance.
- 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 would be dropped because the PBR would have 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

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 3).

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.

Restrictions

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 an customer (IP-based) network into 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 may fail to show all the relevant hop information across the core.

Related Features and Technologies

Information on MPLS Virtual Private Networks (VPNs) is provided in the "MPLS Virtual Private Networks (VPNs)" feature module.

Supported Platforms

The VRF Selection feature is supported on the Cisco 12000 Series router platform. The following list details the supported engines and line cards:

- Engine 0:
  - OC12 PoS
  - 4xOC3 PoS
  - 6/12xDS3 Ocelot
- Engine 2:
  - OC48 PoS
  - 4xOC12 PoS
  - 8/16 OC3 PoS
- Engine 4:
  - 4xOC48 PoS
  - OC192 E4+ PoS

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, see the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS 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

No new or modified RFCs are supported by this feature.

Prerequisites

For the Cisco 12000 Internet router series, the router must contain one of the following line cards:

- Cisco 12000 Internet router series Packet-over-SONET (PoS) Engine 0 OC12 PoS, 4xOC3 PoS or 6/12xDS3 Ocelot line cards. These line cards allow packets designated for the VRF Selection feature to be switched in the software.
- Cisco 12000 Internet router series Packet-over-SONET (PoS) Engine 2 Performance OC48 PoS, 4xOC12 PoS or 8/16 OC3 PoS line cards. These line cards allow packets designated for the VRF Selection feature to be switched in the hardware.
- Cisco 12000 Internet router series Packet-over-SONET (PoS) Engine 4 4xOC48 or OC192 E4+ PoS line cards.

MPLS VPNs must be enabled in the provider network.

Configuration Tasks

See the following sections for configuration tasks for the VRF Selection feature. Each task in the list is identified as either required or optional.

- 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.

	Command	Purpose
Step 1	`Router(config)# vrf selection source source-IP-address source-IP-mask vrf vrf_name`	Populates a single source IP address, or range of source IP addresses, to a VRF Selection table.
Step 2	`Router(config-if)# ip vrf select source`	Enables the VRF Selection feature on an interface.
Step 3	`Router(config-if)# ip vrf receive vrf_name`	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 back 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.

	Command	Purpose
Step 1	`Router(config-if)# ip route vrf vrf_name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]`	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    33.0.0.0/8 [200/0] via 10.10.10.10, 00:00:37
     5.0.0.0/16 is subnetted, 1 subnets
B       5.19.0.0 [200/0] via 10.10.10.10, 00:00:37
     14.0.0.0/32 is subnetted, 1 subnets
B       14.14.14.14 [200/0] via 10.10.10.10, 00:00:37
     15.0.0.0/32 is subnetted, 1 subnets
S       15.15.15.15 [1/0] via 34.0.0.1, 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 2.0.0.0 255.255.0.0 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 2.0.0.0 255.255.0.0 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 2.0.0.0 255.0.0.0 vrf VRF_AOL
    Router(config)#vrf selection source 2.0.0.0 255.0.0.0 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 170.1.2.1 255.255.255.0 vrf red
    % Inconsistent address and mask
    Router(config)#vrf selection source 170.1.2.1 255.255.255.255 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

This section provides the following configuration examples:

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

Enabling MPLS VPNs

The following example enables the router to accept MPLS VPNs:

```
Router(config)# mpls label protocol ldp
Router(config)# interface loopback0
Router(config-if)# ip address 13.13.13.13 255.255.255.255
Router(config-if)# no ip directed-broadcast
```

Creating a VRF Routing Table

The following example creates 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

The following example defines two entries (vpn1 and vpn2) in the VRF Selection table. In this example, packets with the source address of 16.16.0.0 will be routed to the VRF vpn1, and packets with the source address of 17.17.0.0 will be routed to the VRF vpn2:

```
Router(config)# vrf selection source 16.16.0.0 255.255.0.0 vrf vpn1
Router(config)# vrf selection source 17.17.0.0 255.255.0.0 vrf vpn2
```

Defining IP Static Routes for a VRF

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

```
Router(config)# ip route vrf vpn1 16.16.0.0 255.255.0.0 POS1/0
Router(config)# ip route vrf vpn2 17.17.0.0 255.255.0.0 POS1/0
```

Configuring an Interface for VRF Selection

The following example configures the POS1/0 interface for the VRF Selection feature and adds the configured IP address (31.0.0.1) 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 31.0.0.1 255.0.0.0
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

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 11.11.11.11 remote-as 1000
Router(config-router)# neighbor 11.11.11.11 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 11.11.11.11 activate
Router(config-router-af)# neighbor 11.11.11.11 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

If a packet arrives at an interface that has VRF Select enabled, and its source IP address does not match any VRF Select definition, that packet will be forwarded via the global routing table. This default behavior could cause problems if IP address spoofing is being implemented. Unnecessary traffic could be forwarded via 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 dropping the packets.

```
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
```

Command Reference

This section provides new commands. All other commands used with the VRF Selection feature are documented in the Cisco IOS Release 12.0 command reference publications.

New Commands

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

ip vrf receive

To add all the IP addresses that are associated with an interface into a VRF table, use the **ip vrf receive** command in interface configuration mode. To remove the IP addresses from the VRF table, use the **no** form of this command.

ip vrf receive *vrf_name*

no ip vrf receive *vrf_name*

Syntax Description

vrf_name	Name of the VRF table to which the IP addresses of the interface will be added.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

This command adds all the IP addresses that are associated with an interface into a VRF table. These IP address entries will then be inserted as a connected route and will appear as “receive” entries in the CEF table.

Interfaces where the VRF Selection feature is enabled will 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 will, by default, be dropped because there is no corresponding “receive” entry in the VRF CEF entry.

The **ip vrf receive** command allows the IP addresses that are associated with an interface to be inserted as a connected route into a particular VRF. Once the IP addresses are inserted as a connected route, the interface is allowed to respond to requests (such as a ping request) directed to it from a VPN.

This command can be entered once on an interface to add IP addresses to one VRF table, or can be entered multiple times to add the IP addresses to more than one VRF table.

The IP address does not have to be specified in this command; the IP address and any secondary addresses associated with the interface will be automatically entered into the VRF table.

Examples

The following example shows how to add the IP addresses associated with the interface into the VRF table vpn1:

```
Router(config-if)# ip vrf receive vpn1
```

Related Commands

Command	Description
ip vrf select source	Enables VRF Selection on an interface.
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 sub-interface, use the **ip vrf select source** command in interface configuration mode. To disable the VRF Selection feature on a particular interface or sub-interface, 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.

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
```

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.

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
```

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.