MPLS VPN VRF Selection Based on a Source IP Address

The MPLS VPN VRF Selection Based on a Source IP Address feature allows a specified interface on a provider edge (PE) device 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 device to route packets to different VPNs.

The MPLS VPN VRF Selection Based on a Source IP Address feature allows packets arriving on an interface to be switched into the appropriate virtual routing and forwarding (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, this feature is a "one way" feature; it works on packets coming from the end users to the PE device

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 Based on a Source IP Address

- Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) must be enabled in the provider network.
- 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 a Source IP Address

- The MPLS VPN VRF Selection Based on a Source IP Address feature is supported only in Service Provider (-p-) images.
- The Cisco software must support Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), and the provider network must have MPLS Label Distribution Protocol (LDP) installed and running.
- The MPLS VPN VRF Selection Based on a Source IP Address 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 MPLS VPN VRF Selection Based on a Source IP Address criteria for Engine 2 line cards. The performance of this feature can degrade with longer subnet masks (/24 or /32, for example).
- Cisco Express Forwarding must be enabled on any interfaces that have the MPLS VPN VRF Selection Based on a Source IP Address feature enabled. Distributed Cisco Express Forwarding is enabled by default on Cisco 12000 Series Internet routers.
- An IP traceroute command from an MPLS VPN VRF Selection customer edge (CE) device to a typical MPLS VPN VRF CE device works as expected. However, an IP traceroute command from a typical MPLS VPN VRF CE device to an MPLS VPN VRF Selection CE device might fail to show all the relevant hop information across the core.

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

VRF Selection Process

The MPLS VPN VRF Selection Based on a Source IP Address feature uses the process described in this section to route packets from the customer networks to the provider edge (PE) device and into the provider network.

A two-table lookup mechanism is used at the ingress interface of the PE device to determine the routing and forwarding of packets coming from the customer networks, which use IP protocols, to the Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), 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 device (this is the default behavior), or is dropped.

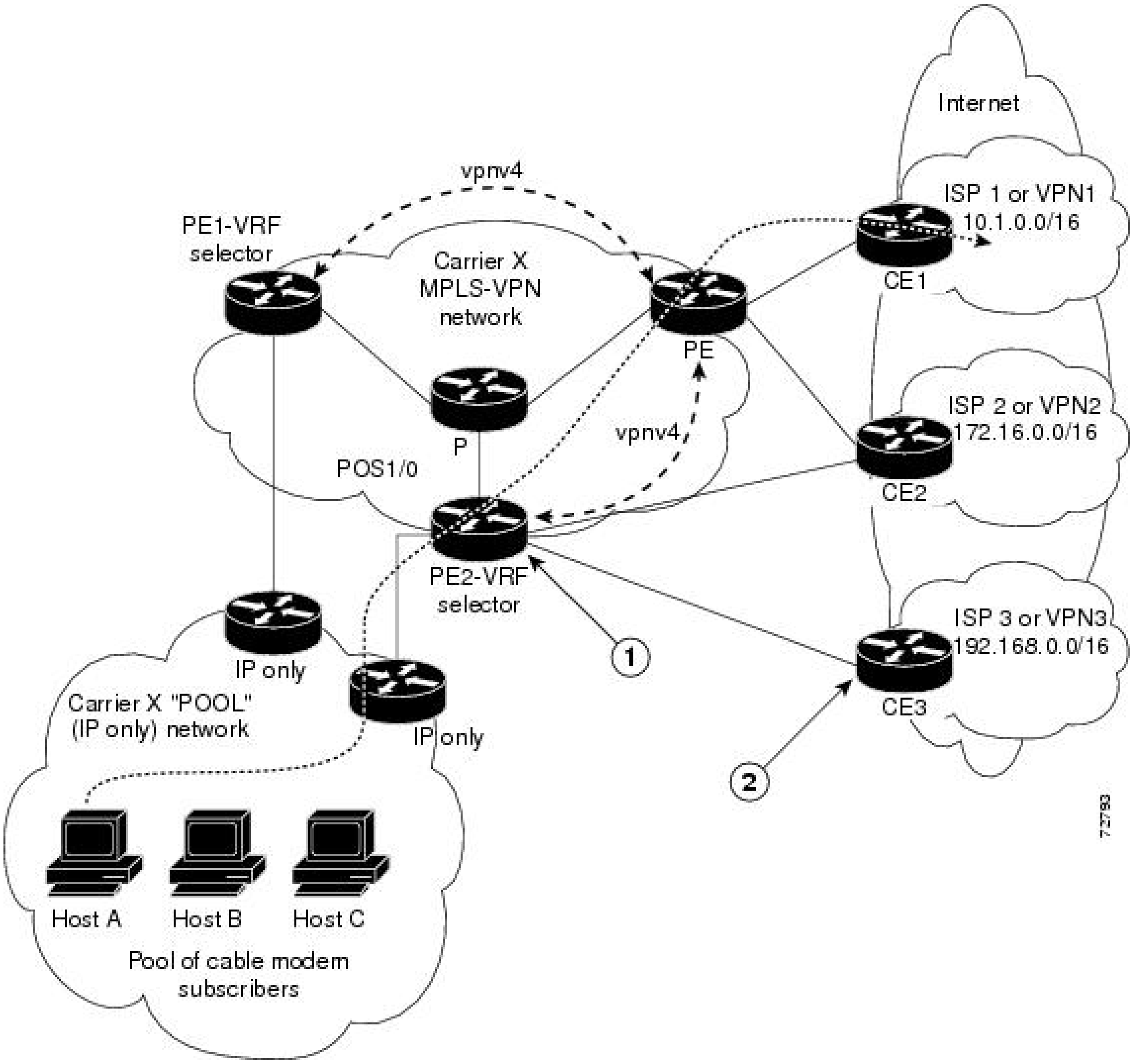
- The second table, the VRF table (also known as the VPN routing table), contains the virtual routing and forwarding information for the specified VPN and is used to forward the selected VPN traffic to the correct MPLS label switched path (LSP) based upon the destination IP address of the packet.

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 MPLS VPN VRF Selection Based on a Source IP Address 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. The figure below provides an example of the MPLS VPN VRF Selection Based on a Source IP Address feature with an IP-based host network, an Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) , 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 device 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 the figure above, 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.

The figure 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 device PE2.

To enable the MPLS VPN VRF Selection Based on a Source IP Address feature on the devices PE1 and PE2, enter the following commands:

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

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 MPLS VPN VRF Selection Based on a Source IP Address 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 MPLS VPN VRF Selection Based on a Source IP Address feature 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 MPLS VPN VRF Selection Based on a Source IP Address feature provides a fast and scalable solution.

VRF Selection is a Unidirectional Feature

In the figure above, the end users are typical Internet home users. If the MPLS VPN VRF Selection Based on a Source IP Address feature were a two-way (bidirectional) feature, traffic coming from the Internet service providers (ISPs) to the hosts would be required to use only the provider edge (PE) devices that have MPLS VPN VRF Selection Based on a Source IP Address feature 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 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) paths, because the VRF Selection-enabled device 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 virtual routing and forwarding (VRF) static routes on the PE device interfaces connected to the ISPs. The VRF static routes would route traffic from the ISPs to the carrier network.

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 MPLS VPN VRF Selection Based on a Source IP Address 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.

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 Internet service providers (ISPs) have provided registered IP address space for all of the subscribed users within the POOL network.

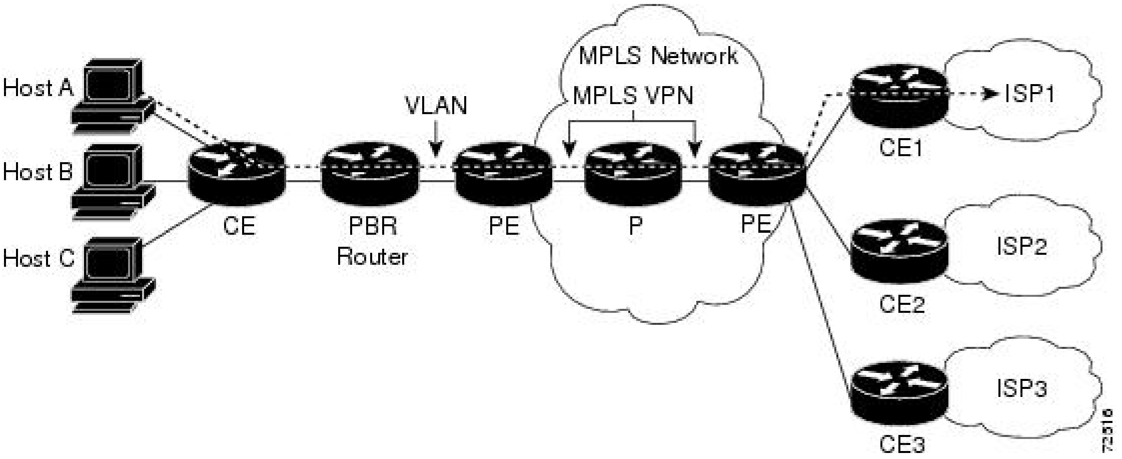
If the POOL network uses IP addresses that are not globally routeable and are designed for a nonconnected enterprise (defined by RFC1918), the MPLS VPN VRF Selection Based on a Source IP Address feature becomes bidirectional. All traffic being sent and received by the host would have to travel via a device that has the MPLS VPN VRF Selection Based on a Source IP Address 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 MPLS VPN VRF Selection Based on a Source IP Address feature removes the association between a Virtual Private Network (VPN) and an interface. Before the MPLS VPN VRF Selection Based on a Source IP Address feature was introduced, the following implementation was used to route outgoing Multiprotocol Label Switching (MPLS) VPN packets to different destinations:

- A policy-based device (PBR) is attached to the customer edge (CE) device.
- The egress side of the PBR device side has VLANs connected to a provider edge (PE) device.
- The PBR device uses a policy-based route map to select the correct output (VLAN) interface, and each VLAN is under a specific VRF. The figure below illustrates a sample configuration in which a PBR device 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 device 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 MPLS VPN VRF Selection Based on a Source IP Address feature addresses the limitations of and problems with using a PBR for packet routing and forwarding.

Benefits of MPLS VPN VRF Selection Based on a Source IP Address

The following are benefits to using the MPLS VPN VRF Selection Based on a Source IP Address method of VPN routing and forwarding.

- Association of VPN to interface is removed—The MPLS VPN VRF Selection Based on a Source IP Address feature removes the association between a Virtual Private Network (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 provider edge (PE) device in the provider network-Access points to each network can be established at any MPLS PE device and can be made redundant by connections to multiple PE devices (for example, the CE2 device in the figure above).

- Multiple points in the provider network can be used for VPN routing and forwarding—MPLS VPNs, like IP, are connectionless. Any PE device, whether MPLS VPN VRF Selection Based on a Source IP Address feature is enabled or not, is capable of carrying VRF Selection traffic from the MPLS network out to the customer edge (CE) devices.

How to Configure MPLS VPN VRF Selection Based on a Source IP Address

Configuring VRF Selection

To add a source IP address to a VRF Selection table, complete the following steps:

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 or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf selection source** *source-ip-address source-ip-mask* **vrf** *vrf-name* **Example:** `Device(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:** `Device(config-if)# ip vrf select source`	Enables the MPLS VPN VRF Selection Based on a Source IP Address feature on an interface.

	Command or Action	Purpose
Step 5	**ip vrf receive** *vrf-name* **Example:** `Device(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 Internet service providers (ISPs) to the hosts does not require the use of the Multiprotocol Label Switching (MPLS) Virtual Private Network (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 MPLS VPN VRF Selection Based on a Source IP Address interface. The remote provider edge (PE) device 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**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# 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**] **Example:** `Device(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 privileged EXEC mode to display the IP routing table associated with a virtual routing and forwarding (VRF) instance. This example shows the IP routing table associated with the VRF vrf1:

```
Device#  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 MPLS VPN VRF Selection Based on a Source IP Address feature.

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

If you attempt to configure a nonexisting MPLS VPN VRF Selection Based on a Source IP Address table, the following error appears:

```
Device(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 an MPLS VPN VRF Selection Based on a Source IP Address entry that does not exist, the following error appears:

```
Device(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 an MPLS VPN VRF Selection Based on a Source IP Address entry, the following error appears:

```
Device(config)# vrf selection source 172.16.0.0 255.0.0.0 vrf VRF_AOL
Device(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 an MPLS VPN VRF Selection Based on a Source IP Address entry, the following error appears:

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

If you attempt to configure a VRF instance on an interface that has MPLS VPN VRF Selection Based on a Source IP Address already configured, the following error appears:

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

To enable VRF, first remove MPLS VPN VRF Selection Based on a Source IP Address from the interface. If you attempt to configure an MPLS VPN VRF Selection Based on a Source IP Address entry on an interface that has VRF already configured, the following error appears:

```
Device(config-if)# ip vrf forward red
Device(config-if)# ip vrf select red
% Can not configure VRF Select if interface is under a non-global VRF
```

To enable the MPLS VPN VRF Selection Based on a Source IP Address feature, first remove VRF from the interface

Configuration Examples for MPLS VPN VRF Selection Based on a Source IP Address

Example: Enabling MPLS VPNs

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

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

Example: Creating a VRF Routing Table

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

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

Example: Defining VRF Selection Entries

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:

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

Example: Defining IP Static Routes for a VRF

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

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

Example: Configuring an Interface for VRF Selection

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

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

Example: Configuring a BGP Device for VRF Selection

A device that is enable with the MPLS VPN VRF Selection Based on a Source IP Address feature requires an MPLS VPN BGP configuration. The following example configures a device that is using BGP for the MPLS VPN VRF Selection Based on a Source IP Address feature:

```
Device(config)# router bgp 1000
Device(config-router)# no bgp default ipv4-unicast
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# timers bgp 10 30
Device(config-router)# neighbor 10.11.11.11 remote-as 1000
Device(config-router)# neighbor 10.11.11.11 update-source Loopback0
Device(config-router)# no auto-summary
Device(config-router)# address-family vpnv4
Device(config-router-af)# neighbor 10.11.11.11 activate
Device(config-router-af)# neighbor 10.11.11.11 send-community extended
Device(config-router-af)# exit-address-family
Device(config-router)# address-family ipv4 vrf vpn2
Device(config-router-af)# redistribute static
Device(config-router-af)# no auto-summary
Device(config-router-af)# no synchronization
Device(config-router-af)# exit-address-family
Device(config-router)# address-family ipv4 vrf vpn1
Device(config-router-af)# redistribute static
Device(config-router-af)# no auto-summary
Device(config-router-af)# no synchronization
Device(config-router-af)# exit-address-family
```

Example: Configuring a VRF to Eliminate Unnecessary Packet Forwarding

If a packet arrives at an interface that has the MPLS VPN VRF Selection Based on a Source IP Address feature 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.

```
Device(config)# ip vrf VRF_DROP
Device(config-vrf)# rd 999:99
Device(config-vrf)# route-target export 999:99
Device(config-vrf)# route-target import 999:99
Device(config-vrf)# exit
Device(config)# vrf selection source 0.0.0.0 0.0.0.0 vrf VRF_DROP
Device(config)# ip route vrf VRF_DROP 0.0.0.0 0.0.0.0 Null0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco Master Command List, All Releases
MPLS and MPLS applications commands	Cisco IOS Multiprotocol Label Switching Command Reference

Technical Assistance

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

Feature Information for MPLS VPN VRF Selection Based on a Source IP Address

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 Based on a Source IP Address

Feature Name	Releases	Feature Information
MPLS VPN VRF Selection Based on a Source IP Address	12.0(22)S 12.0(23)S 12.0(24)S 12.0(26)S 12.2(18)S 12.2(27)SBC	The MPLS VPN VRF Selection Based on a Source IP Address feature allows a specified interface on a provider edge (PE) device 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 device to route packets to different VPNs. In Cisco IOS Release 12.0(22)S, this feature was introduced on the Cisco 12000 Series Internet Router. In Cisco IOS Release 12.0(23)S, this feature was updated to support the 1-port 10-Gigabit Ethernet (E4+), 3-port Gigabit Ethernet , and the Modular Gigabit Ethernet (E4+) line cards. In Cisco IOS Release 12.0(24)S, support for the Cisco 12000 Series Internet Router engine 3 was added. In Cisco IOS Release 12.0(26)S, this feature was implemented on the Cisco 7200 and 7500 series routers. In Cisco IOS Release 12.2(18)S, this feature was implemented on the Cisco 7304 router. In Cisco IOS Release 12.2(27)SBC, this feature was integrated. The following commands were introduced or modified: **ip vrf receive**, **ip vrf select source**, **vrf selection source**.