MPLS Layer 3 VPNs Configuration Guide, Cisco IOS XE Release 2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Configuring MPLS Layer 3 VPNs

A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. This module explains how to create an MPLS VPN.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MPLS Layer 3 VPNs

Before configuring MPLS Layer 3 VPNs, you should have MPLS, Label Distribution Protocol (LDP), and Cisco Express Forwarding installed in your network. All routers in the core, including the PE routers, must be able to support Cisco Express Forwarding and MPLS forwarding. See the Assessing the Needs of MPLS VPN Customers, page 9 for more information.

Cisco Express Forwarding must be enabled all routers in the core, including the PE routers. For information about how to determine if Cisco Express Forwarding is enabled, see Configuring Basic Cisco Express Forwarding--Improving Performance, Scalability, and Resiliency in Dynamic Network .

Restrictions for MPLS Layer 3 VPNs

When configuring static routes in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS XE releases that support the Tag Forwarding Information Base (TFIB). The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS XE releases that support the MPLS Forwarding Infrastructure (MFI). Use the following guidelines when configuring static routes.

Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in MPLS environment:

ip route *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1**

ip route *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

ip route *destination-prefix mask* **next-hop1**

ip route *destination-prefix mask* **next-hop2**

Use the *interface* and *next-hop* arguments when specifying static routes.

Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop and interface are in the same VRF:

- ◦ **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
  ◦ **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
  ◦ **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**
  ◦ **ip route vrf** *vrf-name destination-prefix mask* **interface2 next-hop2**

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet Gateway.

- ◦ **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**

- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address* (This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 next-hop1**

ip route *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS VPN Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

ip route vrf *destination-prefix mask next-hop-address* **global**

The following **ip route** commands are not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

ip route vrf *destination-prefix mask* **next-hop1 global**

ip route vrf *destination-prefix mask* **next-hop2 global**

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

ip route vrf *vrf-name destination-prefix mask* **next-hop1** *vrf-name destination-prefix mask* **next-hop1**

ip route vrf *vrf-name destination-prefix mask* **next-hop2**

Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table on the CE side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGP multihop cases.

ip route vrf *vrf-name destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static non-recursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 nexthop1**

ip route *destination-prefix mask* **interface2 nexthop2**

Information About MPLS Layer 3 VPNs

MPLS VPN Definition

Before defining an MPLS VPN, you need to define a VPN in general. A VPN is:

- An IP-based network delivering private network services over a public infrastructure
- A set of sites that are allowed to communicate with each other privately over the Internet or other public or private networks

Conventional VPNs are created by configuring a full mesh of tunnels or permanent virtual circuits (PVCs) to all sites in a VPN. This type of VPN is not easy to maintain or expand, because adding a new site requires changing each edge device in the VPN.

MPLS-based VPNs are created in Layer 3 and are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without the customer's involvement.

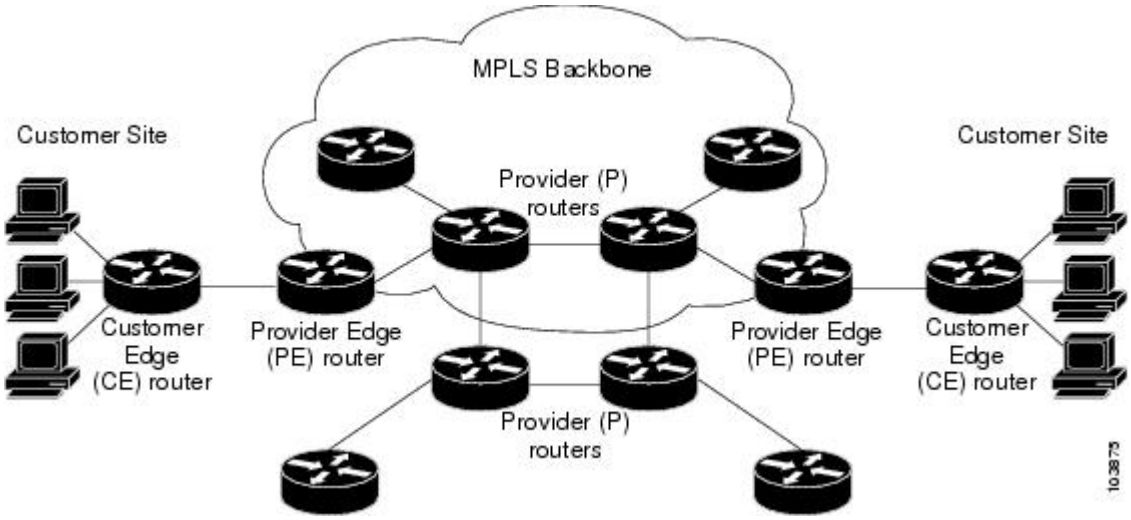
MPLS VPNs are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS VPN, only the service provider’s edge router that provides services to the customer site needs to be updated.

The different parts of the MPLS VPN are described as follows:

- Provider (P) router--Router in the core of the provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS label in each route assigned by the PE router) to routed packets. VPN labels are used to direct data packets to the correct egress router.
- PE router--Router that attaches the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE router attaches directly to a CE router.
- Customer (C) router--Router in the ISP or enterprise network.
- Customer edge router--Edge router on the network of the ISP that connects to the PE router on the network. A CE router must interface with a PE router.

The figure below shows a basic MPLS VPN.

Figure 1 Basic MPLS VPN Terminology



How an MPLS VPN Works

MPLS VPN functionality is enabled at the edge of an MPLS network. The PE router performs the following:

- Exchanges routing updates with the CE router
- Translates the CE routing information into VPNv4 routes
- Exchanges VPNv4 routes with other PE routers through the Multiprotocol Border Gateway Protocol (MP-BGP)

How Virtual Routing and Forwarding Tables Work in an MPLS VPN

Each VPN is associated with one or more virtual routing and forwarding (VRF) instances. A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of the following components:

- An IP routing table
- A derived Cisco Express Forwarding table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocol parameters that control the information that is included in the routing table

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A site can be a member of multiple VPNs. However, a site can associate with only one VRF. A site's VRF contains all the routes available to the site from the VPNs of which it is a member.

Packet forwarding information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of routing and Cisco Express Forwarding tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN, and also prevent packets that are outside a VPN from being forwarded to a router within the VPN.

How VPN Routing Information Is Distributed in an MPLS VPN

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. VPN routing information is distributed as follows:

- When a VPN route that is learned from a CE router is injected into BGP, a list of VPN route target extended community attributes is associated with it. Typically the list of route target community extended values is set from an export list of route targets associated with the VRF from which the route was learned.
- An import list of route target extended communities is associated with each VRF. The import list defines route target extended community attributes that a route must have in order for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target extended communities A, B, and C, then any VPN route that carries any of those route target extended communities--A, B, *or* C--is imported into the VRF.

BGP Distribution of VPN Routing Information

A PE router can learn an IP prefix from the following sources:

- A CE router by static configuration
- A BGP session with the CE router
- A Routing Information Protocol (RIP) exchange with the CE router

The IP prefix is a member of the IPv4 address family. After the PE router learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses. The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the VRF on the PE router.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels:

- Within IP domains, known as an autonomous system (interior BGP [IBGP])
- Between autonomous systems (external BGP [EBGP]).

PE-PE or PE-RR (route reflector) sessions are IBGP sessions, and PE-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (see RFC 2283, Multiprotocol Extensions for BGP-4), which define support for address families other than IPv4. Using the extensions ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

MPLS Forwarding

Based on routing information stored in the VRF IP routing table and VRF Cisco Express Forwarding table, packets are forwarded to their destination using MPLS.

A PE router binds a label to each customer prefix learned from a CE router and includes the label in the network reachability information for the prefix that it advertises to other PE routers. When a PE router forwards a packet received from a CE router across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet, it pops the label and uses it to direct the packet to the correct CE router. Label forwarding across the provider backbone is based on either dynamic label switching or traffic engineered paths. A customer data packet carries two levels of labels when traversing the backbone:

- The top label directs the packet to the correct PE router.
- The second label indicates how that PE router should forward the packet to the CE router.

Major Components of MPLS VPNs

An MPLS-based VPN network has three major components:

- VPN route target communities--A VPN route target community is a list of all members of a VPN community. VPN route targets need to be configured for each VPN community member.
- Multiprotocol BGP (MP-BGP) peering of VPN community PE routers--MP-BGP propagates VRF reachability information to all members of a VPN community. MP-BGP peering needs to be configured in all PE routers within a VPN community.

- MPLS forwarding--MPLS transports all traffic between all VPN community members across a VPN service-provider network.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs. However, a site can associate with only one VRF. A customer-site VRF contains all the routes available to the site from the VPNs of which it is a member.

Benefits of an MPLS VPN

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, such as the following:

Connectionless Service

A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate. To establish privacy in a connectionless IP environment, current VPN solutions impose a connection-oriented, point-to-point overlay on the network. Even if it runs over a connectionless network, a VPN cannot take advantage of the ease of connectivity and multiple services available in connectionless networks. When you create a connectionless VPN, you do not need tunnels and encryption for network privacy, thus eliminating significant complexity.

Centralized Service

Building VPNs in Layer 3 allows delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services. It must also provide a way to flexibly deliver value-added services to targeted customers. Scalability is critical, because customers want to use services privately in their intranets and extranets. Because MPLS VPNs are seen as private intranets, you may use new IP services such as:

- Multicast
- Quality of service (QoS)
- Telephony support within a VPN
- Centralized services including content and web hosting to a VPN

You can customize several combinations of specialized services for individual customers. For example, a service that combines IP multicast with a low-latency service class enables video conferencing within an intranet.

Scalability

If you create a VPN using connection-oriented, point-to-point overlays, Frame Relay, or ATM virtual connections (VCs), the VPN's key deficiency is scalability. Specifically, connection-oriented VPNs without fully meshed connections between customer sites are not optimal. MPLS-based VPNs instead use the peer model and Layer 3 connectionless architecture to leverage a highly scalable VPN solution. The peer model requires a customer site to peer with only one PE router as opposed to all other customer edge (CE) routers that are members of the VPN. The connectionless architecture allows the creation of VPNs in Layer 3, eliminating the need for tunnels or VCs.

Other scalability issues of MPLS VPNs are due to the partitioning of VPN routes between PE routers and the further partitioning of VPN and IGP routes between PE routers and provider (P) routers in a core network.

- PE routers must maintain VPN routes for those VPNs who are members.

- P routers do not maintain any VPN routes.

This increases the scalability of the provider's core and ensures that no one device is a scalability bottleneck.

Security

MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN.

Security is provided in the following areas:

- At the edge of a provider network, ensuring packets received from a customer are placed on the correct VPN.
- At the backbone, VPN traffic is kept separate. Malicious spoofing (an attempt to gain access to a PE router) is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

Easy to Create

To take full advantage of VPNs, customers must be able to easily create new VPNs and user communities. Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required. You can add sites to intranets and extranets and form closed user groups. Managing VPNs in this manner enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets.

Flexible Addressing

To make a VPN service more accessible, customers of a service provider can design their own addressing plan, independent of addressing plans for other service provider customers. Many customers use private address spaces, as defined in RFC 1918, and do not want to invest the time and expense of converting to public IP addresses to enable intranet connectivity. MPLS VPNs allow customers to continue to use their present address spaces without network address translation (NAT) by providing a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate. This enables customers to use their own unregistered private addresses, and communicate freely across a public IP network.

Integrated Quality of Service (QoS) Support

QoS is an important requirement for many IP VPN customers. It provides the ability to address two fundamental VPN requirements:

- Predictable performance and policy implementation
- Support for multiple levels of service in an MPLS VPN

Network traffic is classified and labeled at the edge of the network before traffic is aggregated according to policies defined by subscribers and implemented by the provider and transported across the provider core. Traffic at the edge and core of the network can then be differentiated into different classes by drop probability or delay.

Straightforward Migration

For service providers to quickly deploy VPN services, use a straightforward migration path. MPLS VPNs are unique because you can build them over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks.

Migration for the end customer is simplified because there is no requirement to support MPLS on the CE router and no modifications are required to a customer's intranet.

How to Configure MPLS Layer 3 VPNs

Configuring the Core Network

Assessing the Needs of MPLS VPN Customers

Before you configure an MPLS VPN, you need to identify the core network topology so that it can best serve MPLS VPN customers. Perform this task to identify the core network topology.

SUMMARY STEPS

1. Identify the size of the network.
2. Identify the routing protocols in the core.
3. Determine if you need MPLS VPN High Availability support.
4. Determine if you need BGP load sharing and redundant paths in the MPLS VPN core.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Identify the size of the network.	Identify the following to determine the number of routers and ports you need: • How many customers do you need to support? • How many VPNs are needed per customer? • How many virtual routing and forwarding instances are there for each VPN?
Step 2	Identify the routing protocols in the core.	Determine which routing protocols you need in the core network.
Step 3	Determine if you need MPLS VPN High Availability support.	MPLS VPN Nonstop Forwarding and Graceful Restart are supported on select routers and Cisco software releases. Contact Cisco Support for the exact requirements and hardware support.

	Command or Action	Purpose
Step 4	Determine if you need BGP load sharing and redundant paths in the MPLS VPN core.	See *Load Sharing MPLS VPN Traffic* for configuration steps.

Configuring Routing Protocols in the Core

To configure a routing protocol, such as BGP, OSPF, IS-IS, EIGRP,and static, see the following documents:

- Configuring BGP
- Configuring OSPF
- Configuring IS-IS
- Configuring ERGRP
- Configuring static routes

Configuring MPLS in the Core

To enable MPLS on all routers in the core, you must configure a label distribution protocol. You can use either of the following as a label distribution protocol:

- MPLS Label Distribution Protocol (LDP). For configuration information, see the MPLS Label Distribution Protocol (LDP).
- MPLS Traffic Engineering Resource Reservation Protocol (RSVP). For configuration information, see MPLS Traffic Engineering and Enhancements.

Configuring Multiprotocol BGP on the PE Routers and Route Reflectors

Perform this task to configure multiprotocol BGP (MP-BGP) connectivity on the PE routers and route reflectors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **address-family vpnv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-number* **Example:** `Router(config)# router bgp 100`	Configures a BGP routing process and enters router configuration mode. • The *as-number* argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.
Step 4	**no bgp default ipv4-unicast** **Example:** `Router(config-router)# no bgp default ipv4-unicast`	(Optional) Disables the IPv4 unicast address family on all neighbors. • Use the **no bgp default ipv4-unicast** command if you are using this neighbor for MPLS routes only.
Step 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* **Example:** `Router(config-router)# neighbor 10.0.0.1 remote-as 100`	Adds an entry to the BGP or multiprotocol BGP neighbor table. • The *ip-address* argument specifies the IP address of the neighbor. • The *peer-group-name* argument specifies the name of a BGP peer group. • The *as-number* argument specifies the autonomous system to which the neighbor belongs.
Step 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** **Example:** `Router(config-router)# neighbor 10.0.0.1 activate`	Enables the exchange of information with a neighboring BGP router. • The *ip-address* argument specifies the IP address of the neighbor. • The *peer-group-name* argument specifies the name of a BGP peer group.

	Command or Action	Purpose
Step 7	**address-family vpnv4** [**unicast**] **Example:** `Router(config-router)# address-family vpnv4`	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. • The optional **unicast** keyword specifies VPNv4 unicast address prefixes.
Step 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** **Example:** `Router(config-router-af)# neighbor 10.0.0.1 send-community extended`	Specifies that a communities attribute should be sent to a BGP neighbor. • The *ip-address* argument specifies the IP address of the BGP-speaking neighbor. • The *peer-group-name* argument specifies the name of a BGP peer group.
Step 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.1 activate`	Enables the exchange of information with a neighboring BGP router. • The *ip-address* argument specifies the IP address of the neighbor. • The *peer-group-name* argument specifies the name of a BGP peer group.
Step 10	**end** **Example:** `Router(config-router-af)# end`	(Optional) Exits to privileged EXEC mode.

- Troubleshooting Tips, page 12

Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command is not successful, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

Connecting the MPLS VPN Customers

- Defining VRFs on the PE Routers to Enable Customer Connectivity, page 12
- Configuring VRF Interfaces on PE Routers for Each VPN Customer, page 14

Defining VRFs on the PE Routers to Enable Customer Connectivity

To define VPN routing and forwarding (VRF) instances, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map** *route-map*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf vpn1`	Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode. • The *vrf-name* argument is the name assigned to a VRF.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables. • The *route-distinguisher* argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats: ◦ 16-bit AS number: your 32-bit number, for example, 101:3 ◦ 32-bit IP address: your 16-bit number, for example, 10.0.0.1:1

	Command or Action	Purpose
Step 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf)# route-target import 100:1`	Creates a route-target extended community for a VRF. • The **import** keyword imports routing information from the target VPN extended community. • The **export** keyword exports routing information to the target VPN extended community. • The **both** keyword imports routing information from and exports routing information to the target VPN extended community. • The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.
Step 6	**import map** *route-map* **Example:** `Router(config-vrf)# import map vpn1-route-map`	(Optional) Configures an import route map for a VRF. • The *route-map* argument specifies the route map to be used as an import route map for the VRF.
Step 7	**exit** **Example:** `Router(config-vrf)# exit`	(Optional) Exits to global configuration mode.

Configuring VRF Interfaces on PE Routers for Each VPN Customer

To associate a VRF with an interface or subinterface on the PE routers, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 1/0/0`	Specifies the interface to configure and enters interface configuration mode. • The *type* argument specifies the type of interface to be configured. • The *number* argument specifies the port, connector, or interface card number.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding vpn1`	Associates a VRF with the specified interface or subinterface. • The *vrf-name* argument is the name assigned to a VRF.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Exits to privileged EXEC mode.

Configuring Routing Protocols Between the PE and CE Routers

Configure the PE router with the same routing protocol that the CE router uses. You can configure the following routing protocols:

- Configuring BGP as the Routing Protocol Between the PE and CE Routers, page 15
- Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers, page 17
- Configuring Static Routes Between the PE and CE Routers, page 19
- Configuring OSPF as the Routing Protocol Between the PE and CE Routers, page 21
- Configuring EIGRP as the Routing Protocol Between the PE and CE Routers, page 23
- Configuring EIGRP Redistribution in the MPLS VPN, page 26

Configuring BGP as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions using BGP, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **exit-address-family**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-number* **Example:** `Router(config)# router bgp 100`	Configures a BGP routing process and enters router configuration mode. • The *as-number* argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.
Step 4	**address-family ipv4** [**multicast**	**unicast**	**vrf** *vrf-name*] **Example:** `Router(config-router)# address-family ipv4 vrf vpn1`	Specifies the IPv4 address family type and enters address family configuration mode. • The **multicast** keyword specifies IPv4 multicast address prefixes. • The **unicast** keyword specifies IPv4 unicast address prefixes. • The **vrf** *vrf-name* keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.

	Command or Action	Purpose
Step 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* **Example:** `Router(config-router-af)# neighbor 10.0.0.1 remote-as 200`	Adds an entry to the BGP or multiprotocol BGP neighbor table. • The *ip-address* argument specifies the IP address of the neighbor. • The *peer-group-name* argument specifies the name of a BGP peer group. • The *as-number* argument specifies the autonomous system to which the neighbor belongs.
Step 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.1 activate`	Enables the exchange of information with a neighboring BGP router. • The *ip-address* argument specifies the IP address of the neighbor. • The *peer-group-name* argument specifies the name of a BGP peer group.
Step 7	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode.
Step 8	**end** **Example:** `Router(config-router)# end`	(Optional) Exits to privileged EXEC mode.

Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions using RIPv2, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** {**1** | **2**}
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **network** *ip-address*
7. **redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
8. **exit-address-family**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router rip** **Example:** `Router(config)# router rip`	Enables RIP.
Step 4	**version** {**1** | **2**} **Example:** `Router(config-router)# version 2`	Specifies a Routing Information Protocol (RIP) version used globally by the router.
Step 5	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] **Example:** `Router(config-router)# address-family ipv4 vrf vpn1`	Specifies the IPv4 address family type and enters address family configuration mode. • The **multicast** keyword specifies IPv4 multicast address prefixes. • The **unicast** keyword specifies IPv4 unicast address prefixes. • The **vrf** *vrf-name* keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.
Step 6	**network** *ip-address* **Example:** `Router(config-router-af)# network 192.168.7.0`	Enables RIP on the PE-to-CE link.

	Command or Action	Purpose
Step 7	**redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router-af)# redistribute bgp 200`	Redistributes routes from one routing domain into another routing domain. • For the RIPv2 routing protocol, use the **redistribute bgp** *as-number* command.
Step 8	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode.
Step 9	**end** **Example:** `Router(config-router)# end`	(Optional) Exits to privileged EXEC mode.

Configuring Static Routes Between the PE and CE Routers

To configure PE-to-CE routing sessions that use static routes, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route vrf** *vrf-name*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
6. **redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
7. **exit-address-family**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip route vrf** *vrf-name* **Example:** `Router(config)# ip route vrf 200`	Defines static route parameters for every PE-to-CE session.
Step 4	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] **Example:** `Router(config-router)# address-family ipv4 vrf vpn1`	Specifies the IPv4 address family type and enters address family configuration mode. • The **multicast** keyword specifies IPv4 multicast address prefixes. • The **unicast** keyword specifies IPv4 unicast address prefixes. • The **vrf** *vrf-name* keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.
Step 5	**redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router-af)# redistribute static`	Redistributes routes from one routing domain into another routing domain. • To redistribute VRF static routes into the VRF BGP table, use the **redistribute static** command. See the command for information about other arguments and keywords.

	Command or Action	Purpose
Step 6	**redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router-af)# redistribute connected`	Redistributes routes from one routing domain into another routing domain. • To redistribute directly connected networks into the VRF BGP table, use the **redistribute connected** command.
Step 7	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode.
Step 8	**end** **Example:** `Router(config-router)# end`	(Optional) Exits to privileged EXEC mode.

Configuring OSPF as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions that use OSPF, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **network** *ip-address wildcard-mask* **area** *area-id*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
7. **exit-address-family**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 1 vrf grc`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process. • The **vrf** *vpn-name* keyword and argument identify a VPN. Create a separate OSPF process for each VRF that will receive VPN routes.
Step 4	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(config-router)# network 10.0.0.1 0.0.0.3 area 20`	Defines the interfaces on which OSPF runs and to defines the area ID for those interfaces. • The *ip-address* argument identifies the IP address. • The *wildcard-mask* argument identifies the IP-address-type mask that includes “don't care” bits. • The *area-id* argument identifies the area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. To associate areas with IP subnets, specify a subnet address as the value of the *area-id*argument.
Step 5	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] **Example:** `Router(config-router)# address-family ipv4 vrf vpn1`	Specifies the IPv4 address family type and enters address family configuration mode. • The **multicast** keyword specifies IPv4 multicast address prefixes. • The **unicast** keyword specifies IPv4 unicast address prefixes. • The **vrf** *vrf-name* keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.

	Command or Action	Purpose
Step 6	**redistribute** *protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router-af)#  redistribute rip metric 1 subnets`	Redistributes routes from one routing domain into another routing domain. You may need to include several protocols to ensure that all IBGP routes are distributed into the VRF.
Step 7	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode.
Step 8	**end** **Example:** `Router(config-router)# end`	(Optional) Exits to privileged EXEC mode.

Configuring EIGRP as the Routing Protocol Between the PE and CE Routers

Using Enhanced Interior Gateway Routing Protocol (EIGRP) between the PE and CE routers allows you to transparently connect EIGRP customer networks through an MPLS-enabled BGP core network so that EIGRP routes are redistributed through the VPN across the BGP network as internal BGP (iBGP) routes.

To configure PE-to-CE routing sessions that use EIGRP, perform this task.

BGP must be configured in the network core.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no synchronization**
5. **neighbor** *ip-address* **remote-as** *as-number*
6. **neighbor** *ip-address update-source* **loopback** *interface-number*
7. **address-family vpnv4**
8. **neighbor** *ip-address* **activate**
9. **neighbor** *ip-address* **send-community extended**
10. **exit-address-family**
11. **address-family ipv4 vrf** *vrf-name*
12. **redistribute eigrp** *as-number* [**metric** *metric-value*] [**route-map** *map-name*]
13. **no synchronization**
14. **exit-address-family**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-number* **Example:** `Router(config)# router bgp 10`	Enters router configuration mode, and creates a BGP routing process.
Step 4	**no synchronization** **Example:** `Router(config-router)# no synchronization`	Configures BGP to send advertisements without waiting to synchronize with the IGP.

	Command or Action	Purpose
Step 5	**neighbor** *ip-address* **remote-as** *as-number* **Example:** `Router(config-router)# neighbor 10.0.0.1 remote-as 10`	Establishes peering with the specified neighbor or peer-group. • In this step, you are establishing an iBGP session with the PE router that is connected to the CE router at the other CE site.
Step 6	**neighbor** *ip-address update-source* **loopback** *interface-number* **Example:** `Router(config-router)# neighbor 10.0.0.1 update-source loopback 0`	Configures BGP to use any operational interface for TCP connections. • This configuration step is not required. However, the BGP routing process will be less susceptible to the affects of interface or link flapping.
Step 7	**address-family vpnv4** **Example:** `Router(config-router)# address-family vpnv4`	Enters address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes, such as BGP, RIP, and static routing sessions.
Step 8	**neighbor** *ip-address* **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.1 activate`	Establishes peering with the specified neighbor or peer-group. • In this step, you are activating the exchange of VPNv4 routing information between the PE routers.
Step 9	**neighbor** *ip-address* **send-community extended** **Example:** `Router(config-router-af)# neighbor 10.0.0.1 send-community extended`	Configures the local router to send extended community attribute information to the specified neighbor. • This step is required for the exchange of EIGRP extended community attributes.
Step 10	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode and enters router configuration mode.

	Command or Action	Purpose
Step 11	**address-family ipv4 vrf** *vrf-name* **Example:** `Router(config-router)# address-family ipv4 vrf RED`	Configures an IPv4 address-family for the EIGRP VRF and enters address family configuration mode. • An address-family VRF needs to be configured for each EIGRP VRF that runs between the PE and CE routers.
Step 12	**redistribute eigrp** *as-number* [**metric** *metric-value*] [**route-map** *map-name*] **Example:** `Router(config-router-af)# redistribute eigrp 101`	Redistributes the EIGRP VRF into BGP. • The autonomous system number from the CE network is configured in this step.
Step 13	**no synchronization** **Example:** `Router(config-router-af)# no synchronization`	Configures BGP to send advertisements without waiting to synchronize with the IGP.
Step 14	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode and enters router configuration mode.
Step 15	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and enters privileged EXEC mode.

Configuring EIGRP Redistribution in the MPLS VPN

Perform this task to every PE router that provides VPN services to enable EIGRP redistribution in the MPLS VPN.

The metric must be configured for routes from external EIGRP autonomous systems and non-EIGRP networks before these routes can be redistributed into an EIGRP CE router. The metric can be configured in the redistribute statement using the redistribute (IP) command or configured with the default-metric (EIGRP) command. If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route will not be advertised to the CE router.

Note Redistribution between native EIGRP VRFs is not supported. This is designed behavior.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **network** *ip-address wildcard-mask*
6. **redistribute bgp** {*as-number*} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map-name*]
7. **autonomous-system** *as-number*
8. **exit-address-family**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 1`	Enters router configuration mode and creates an EIGRP routing process. • The EIGRP routing process for the PE router is created in this step.
Step 4	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] **Example:** `Router(config-router)# address-family ipv4 vrf RED`	Enters address-family configuration mode and creates a VRF. • The VRF name must match the VRF name that was created in the previous section.

	Command or Action	Purpose
Step 5	**network** *ip-address wildcard-mask* **Example:** `Router(config-router-af)# network 172.16.0.0 0.0.255.255`	Specifies the network for the VRF. • The network statement is used to identify which interfaces to include in EIGRP. The VRF must be configured with addresses that fall within the wildcard-mask range of the network statement.
Step 6	**redistribute bgp** {*as-number*} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map-name*] **Example:** `Router(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500`	Redistributes BGP into the EIGRP. • The autonomous system number and metric of the BGP network is configured in this step. BGP must be redistributed into EIGRP for the CE site to accept the BGP routes that carry the EIGRP information. A metric must also be specified for the BGP network and is configured in this step.
Step 7	**autonomous-system** *as-number* **Example:** `Router(config-router-af)# autonomous-system 101`	Specifies the autonomous system number of the EIGRP network for the customer site.
Step 8	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode and enters router configuration mode.
Step 9	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and enters privileged EXEC mode.

Verifying the VPN Configuration

A route distinguisher must be configured for the VRF, and MPLS must be configured on the interfaces that carry the VRF. Use the **show ip vrf** command to verify the route distinguisher (RD) and interface that are configured for the VRF.

SUMMARY STEPS

1. **show ip vrf**

DETAILED STEPS

show ip vrf
Use this command to display the set of defined VRF instances and associated interfaces. The output also maps the VRF instances to the configured route distinguisher.

Verifying Connectivity Between MPLS VPN Sites

To verify that the local and remote CE routers can communicate across the MPLS core, perform the following tasks:

- Verifying IP Connectivity from CE Router to CE Router Across the MPLS Core, page 29
- Verifying that the Local and Remote CE Routers Are in the Routing Table, page 30

Verifying IP Connectivity from CE Router to CE Router Across the MPLS Core

Perform this task to verify IP connectivity from CE router to CE router across the MPLS VPN.

SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

DETAILED STEPS

Step 1 **enable**
Use this command to enable privileged EXEC mode.

Step 2 **ping** [*protocol*] {*host-name* | *system-address*}
Use this command to diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. Use the **ping** command to verify the connectivity from one CE router to another.

Step 3 **trace** [*protocol*] [*destination*]
Use this command to discover the routes that packets take when traveling to their destination. Use the **trace** command to verify the path that a packet goes through before reaching the final destination. The **trace** command can help isolate a trouble spot if two routers cannot communicate.

Step 4 **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* |*access-list-number*]
Use this command to display the current state of the routing table. Use the *ip-address* argument to verify that CE1 has a route to CE2. Verify the routes learned by CE1. Make sure that the route for CE2 is listed.

Verifying that the Local and Remote CE Routers Are in the Routing Table

Perform this task to check that the local and remote CE routers are in the routing table of the PE routers.

SUMMARY STEPS

1. **enable**
2. **show ip route vrf** *vrf-name* [*prefix*]
3. **show ip cef vrf** *vrf-name* [*ip-prefix*]
4. **exit**

DETAILED STEPS

Step 1 **enable**
Use this command to enable privileged EXEC mode.

Step 2 **show ip route vrf** *vrf-name* [*prefix*]
Use this command to display the IP routing table associated with a VRF. Check that the loopback addresses of the local and remote CE routers are in the routing table of the PE routers.

Step 3 **show ip cef vrf** *vrf-name* [*ip-prefix*]
Use this command to display the Cisco Express Forwarding forwarding table associated with a VRF. Check that the prefix of the remote CE router is in the Cisco Express Forwarding table.

Step 4 **exit**

Configuration Examples for MPLS VPNs

Configuring an MPLS VPN Using BGP Example

This example shows an MPLS VPN that is configured using BGP.

PE Configuration	CE Configuration
ip vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 10.0.0.2 255.0.0.0 no cdp enable ! interface FastEthernet 1/1/0 ip address 10.0.0.1 255.0.0.0 mpls label protocol ldp mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 10.0.0.0 0.255.255.255 area 100 ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected neighbor 10.0.0.1 remote-as 200 neighbor 10.0.0.1 activate neighbor 10.0.0.1 as-override neighbor 10.0.0.1 advertisement-interval 5 no auto-summary no synchronization exit-address-family	ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0 ip address 10.0.0.1 255.0.0.0 no cdp enable ! router bgp 200 bgp log-neighbor-changes neighbor 10.0.0.2 remote-as 100 ! address-family ipv4 redistribute connected neighbor 10.0.0.2 activate neighbor 10.0.0.2 advertisement-interval 5 no auto-summary no synchronization exit-address-family

Configuring an MPLS VPN Using RIP Example

This example shows an MPLS VPN that is configured using RIP.

PE Configuration	CE Configuration
ip vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 10.0.0.2 255.0.0.0 no cdp enable interface FastEthernet 1/1/0 ip address 10.0.0.1 255.0.0.0 mpls label protocol ldp mpls ip ! router rip version 2 timers basic 30 60 60 120 ! address-family ipv4 vrf vpn1 version 2 redistribute bgp 100 metric transparent network 10.0.0.0 distribute-list 20 in no auto-summary exit-address-family ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute rip no auto-summary no synchronization exit-address-family	ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0/0 ip address 10.0.0.1 255.0.0.0 no cdp enable router rip version 2 timers basic 30 60 60 120 redistribute connected network 10.0.0.0 network 10.0.0.1 no auto-summary

Configuring an MPLS VPN Using Static Routes Example

This example shows an MPLS VPN that is configured using static routes.

PE Configuration	CE Configuration
ip vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 10.0.0.2 255.0.0.0 no cdp enable ! interface FastEthernet1/1/0 ip address 10.0.0.1 255.0.0.0 mpls label protocol ldp mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 10.0.0.0 0.255.255.255 area 100 ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute static no auto-summary no synchronization exit-address-family ! ip route vrf vpn1 10.0.0.9 255.255.255.255 10.0.0.1 ip route vrf vpn1 10.0.0.0 255.0.0.0 10.0.0.1	ip cef ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0/0 ip address 10.0.0.1 255.0.0.0 no cdp enable ! ip route 10.0.0.9 255.255.255.255 10.0.0.2 3 ip route 10.0.0.0 255.0.0.0 10.0.0.2 3

Configuring an MPLS VPN Using OSPF Example

This example shows an MPLS VPN that is configured using OSPF.

PE Configuration	CE Configuration
ip vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 10.0.0.2 255.0.0.0 no cdp enable ! router ospf 1000 vrf vpn1 log-adjacency-changes redistribute bgp 100 metric-type 1 subnets network 10.0.0.13 0.0.0.0 area 10000 network 10.0.0.0 0.255.255.255 area 10000 ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute ospf 1000 match internal external 1 external 2 no auto-summary no synchronization exit-address-family	ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0/0 ip address 10.0.0.1 255.0.0.0 no cdp enable ! router ospf 1000 log-adjacency-changes auto-cost reference-bandwidth 1000 redistribute connected subnets network 10.0.0.0 0.255.255.255 area 1000 network 10.0.0.0 0.0.0.0 area 1000

Configuring an MPLS VPN Using EIGRP Example

This example shows an MPLS VPN that is configured using EIGRP.

PE Configuration	CE Configuration
ip vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 interface FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 10.0.0.2 255.0.0.0 no cdp enable interface FastEthernet1/1/0 ip address 10.0.0.1 255.0.0.0 mpls label protocol ldp mpls ip router eigrp 1000 auto-summary ! address-family ipv4 vrf vpn1 redistribute bgp 100 metric 10000 100 255 1 1500 network 10.0.0.0 distribute-list 20 in no auto-summary autonomous-system 1000 exit-address-family ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute eigrp no auto-summary no synchronization exit-address-family	ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0/0 ip address 10.0.0.1 255.0.0.0 no cdp enable ! router eigrp 1000 network 10.0.0.0 auto-summary

Additional References

Related Documents

Related Topic	Document Title
Description of commands associated with MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2283	*Multiprotocol Extensions for BGP-4*
RFC 4364	*BGP/MPLS IP Virtual Private Networks (VPNs)*

Technical Assistance

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

Feature Information for MPLS Layer 3 VPNs

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 Layer 3 VPNs

Feature Name	Releases	Feature Information
MPLS Virtual Private Networks	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	This feature allows a set of sites that to be interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS VPN-OSPF PE-CE Support	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge	Cisco IOS XE Release 2.1	This feature allows you to connect customers running EIGRP to an MPLS VPN.
VPN Routing/Forwarding (VRF) ARP Entry Support	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Multi-protocol BGP (MP-BGP)-MPLS VPN	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	This feature was introduced on Cisco ASR 1000 Series Routers. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

Assigning an ID Number to a VPN

You can identify Virtual Private Networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About VPN ID

Introduction to VPN ID

You can identify VPNs by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN. The VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with VPN ID numbers in the MP-BGP VPNv4 routing updates.

Multiple VPNs can be configured in a router. A VPN is private and uses a private address space that might also be used by another VPN or by the Internet. The IP address used in a VPN is only significant to the VPN in which it exists. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The

VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

Note Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the router. The VPN name is not affected by the VPN ID configuration. These are two independent mechanisms to identify VPNs.

Components of the VPN ID

Each VPN ID defined by RFC 2685 consists of the following elements:

- An Organizational Unique Identifier (OUI), a three-octet hex number: The IEEE Registration Authority assigns OUIs to any company that manufactures components under the ISO/IEC 8802 standard. The OUI is used to generate universal LAN MAC addresses and protocol identifiers for use in local and metropolitan area network applications. For example, an OUI for Cisco Systems is 00-03-6B (hex).
- A VPN index: a four-octet hex number, which identifies the VPN within the company.

Use the following **vpn id** command and specify the VPN ID:

vpn id *oui*:*vpn-index*

A colon separates the OUI from the VPN index.

Management Applications That Use VPN IDs

You can use several applications to manage VPNs by VPN ID. Remote access applications, such as the Remote Authentication Dial-In User Service (RADIUS) and Dynamic Host Configuration Protocol (DHCP), can use the VPN ID feature to identify a VPN. RADIUS can use the VPN ID to assign dial-in users to the proper VPN, based on each user's authentication information.

- Dynamic Host Configuration Protocol, page 40
- Remote Authentication Dial-In User Service, page 40

Dynamic Host Configuration Protocol

Using DHCP network administrators can centrally manage and automate the assignment of IP addresses in an organization's network. The DHCP application uses the VPN ID as follows:

1. A VPN DHCP client requests a connection to a provider edge (PE) router from a VRF interface.
2. The PE router determines the VPN ID associated with that interface.
3. The PE router sends a request with the VPN ID and other information for assigning an IP address to the DHCP server.
4. The DHCP server uses the VPN ID and IP address information to process the request.
5. The DHCP server sends a response back to the PE router, allowing the VPN DHCP client access to the VPN.

Remote Authentication Dial-In User Service

A RADIUS server (or daemon) provides authentication and accounting services to one or more client network access servers (NASs). RADIUS servers authenticate users and return all configuration information necessary for the client to deliver service to the users.

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server.

- The Access-Request packet contains the username, encrypted password, NAS IP address, VPN ID, and port. The format of the request also provides information on the type of session that the user wants to initiate.
- The RADIUS server returns an Access-Accept response if it finds the username and verifies the password. The response includes a list of attribute-value pairs that describe the parameters to be used for this session. If the user is not authenticated, an Access-Reject is sent by the RADIUS server and access is denied.

How to Configure a VPN ID

Specifying a VPN ID

Use this procedure to specify a VPN ID.

Restrictions

The VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with VPN ID numbers in the MP-BGP VPNv4 routing updates.

Each VRF configured on a PE router can have a VPN ID configured. Configure all the PE routers that belong to the same VPN with the same VPN ID. Make sure the VPN ID is unique to the service provider network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **vpn id** *oui*:*vpn-index* :

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf vrf1`	Creates a VRF routing table and a CEF forwarding table and enters VRF configuration mode. • *vrf-name* --Name assigned to a VRF.
Step 4	**vpn id** *oui*:*vpn-index* : **Example:** `Router(config-vrf)# vpn id a1:3f6c`	Assigns the VPN ID to the VRF. • *oui* :--An organizationally unique identifier. The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets. • *vpn-index*--This value identifies the VPN within the company. This VPN index is restricted to four octets.

Verifying the VPN ID Configuration

To verify the VPN ID configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show ip vrf**
3. **show ip vrf id**
4. **show ip vrf detail**

DETAILED STEPS

Step 1 **enable**

Step 2 **show ip vrf**

Use this command to display information about the VRF tables on the PE router. This example displays three VRF tables called vpn1, vpn2, and vpn5.

Example:

```
Router# show ip vrf
  Name                             Default RD          Interfaces
  vpn1                             100:1               FastEthernet1/1/1
                                                       FastEthernet1/0/0
  vpn2                             <not set>
  vpn5                             500:1               Loopback2
```

Step 3 **show ip vrf id**

Use this command to ensure that the PE router contains the VPN ID you specified. The following example shows that only VRF tables vpn1 and vpn2 have VPN IDs assigned. The VRF table called vpn5 is not displayed, because it does not have a VPN ID.

Example:

```
Router# show ip vrf id
VPN Id          Name                             RD
2:3             vpn2                             <not set>
A1:3F6C         vpn1                             100:1
```

Step 4 **show ip vrf detail**

Use this command to see all the VRFs on a PE router. This command displays all the VPN IDs that are configured on the router, their associated VRF names, and VRF route distinguishers (RDs). If a VRF table in the PE router has not been assigned a VPN ID, that VRF entry is not included in the output.

Example:

```
Router# show ip vrf detail
VRF vpn1; default RD 100:1; default VPNID A1:3F6C
  Interfaces:
    FastEthernet1/1/1       FastEthernet1/0/1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                RT:500:1
  No import route-map
  No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
  No interfaces
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
  Interfaces:
```

Configuration Examples for Assigning an ID Number to a VPN

Specifying a VPN ID Example

The following example specifies the VPN ID assigned to the VRF table called vpn1:

```
Router# configure terminal
Router(config)# ip vrf vpn1
Router(config-vrf)# vpn id a1:3f6c
```

Verifying the VPN ID Configuration Example

The following is sample output of the **show ip vrf detail** command, one of the commands that can be used to verify the VPN ID configuration. Use this command to see all the VRFs on a PE router. This command displays all the VPN IDs that are configured on the router, their associated VRF names, and VRF route distinguishers (RDs). If a VRF table in the PE router has not been assigned a VPN ID, that VRF entry is not included in the output.

```
Router# show ip vrf detail
VRF vpn1; default RD 100:1; default VPNID A1:3F6C
  Interfaces:
    FastEthernet1/1/1       FastEthernet1/0/1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                RT:500:1
  No import route-map
  No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
  No interfaces
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
  Interfaces:
```

Additional References

Related Documents

Related Topic	Document Title
Description of commands associated with MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Command Reference*
Basic MPLS VPNs	Configuring MPLS Layer 3 VPNs

Standards

Standard	Title
IEEE Std 802-1990	*IEEE Local and Metropolitan Area Networks: Overview and Architecture*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2685	*Virtual Private Networks Identifier*

Technical Assistance

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

Feature Information for Assigning an ID Number to a VPN

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 2 Feature Information for Assigning an ID Number to a VPN

Feature Name	Releases	Feature Configuration Information
MPLS VPN ID	Cisco IOS XE Release 2.1	You can identify VPNs by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Remote Access MPLS-VPNs

The Remote Access MPLS-VPNs feature allows the service provider to offer a scalable end-to-end Virtual Private Network (VPN) service to remote users. This feature integrates the Multiprotocol Label Switching (MPLS)-enabled backbone with broadband access capabilities.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Remote Access MPLS-VPNs

The Remote Access MPLS-VPNs feature has the following prerequisites:

- Your network must be running the following Cisco IOS XE services before you configure VPN operation:
  - MPLS in the service provider backbone routers
  - Tag Distribution Protocol (TDP) or the Label Distribution Protocol (LDP)
  - Border Gateway Protocol (BGP) in all routers providing a VPN service
  - Cisco Express Forwarding switching in each MPLS-enabled router
- The provider edge (PE) routers that belong to the same VPN must be configured with the same VPN ID. The VPN ID must be unique to the service provider network.

Restrictions for Remote Access MPLS-VPNs

The Remote Access MPLS-VPNs feature has the following restrictions:

- The VPN ID is not used to control the distribution of routing information or to associate IP addresses.

Information About Remote Access MPLS-VPNs

Introduction to Remote Access MPLS-VPNs

MPLS-based VPNs allow service providers to deploy a scalable and cost-effective VPN service that provides a stable and secure path through the network. An enterprise connects to geographically dispersed sites in the Internet service provider's (ISPs) network through use of an MPLS backbone. Sites are interconnected to create an MPLS VPN.

The Remote Access MPLS-VPNs feature allows the service provider to offer a scalable end-to-end VPN service to remote users. The Remote Access MPLS-VPNs feature integrates the MPLS-enabled backbone with broadband access capabilities. By integrating access VPNs with MPLS VPNs, a service provider can:

- Enable remote users and offices to seamlessly access their corporate networks
- Offer equal access to a set of different ISPs or retail service providers
- Integrate their broadband access networks with the MPLS-enabled backbone
- Provide end-to-end VPN service to enterprise customers with remote access (RA) users and offices
- Separate network access and connectivity functions from ISP functions

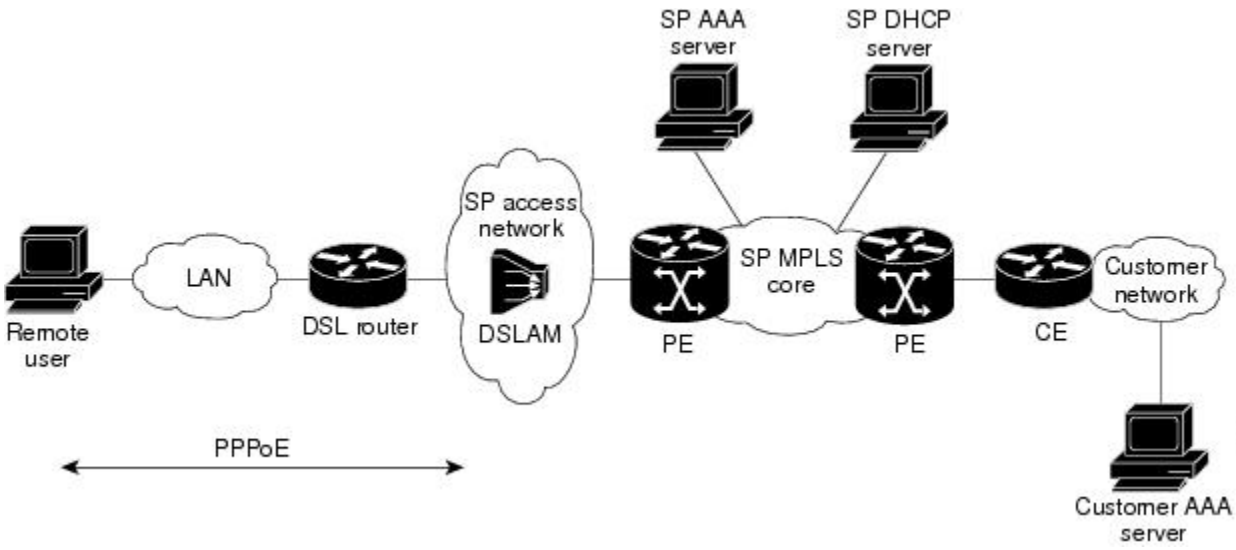
MPLS VPN Architecture

MPLS VPN architecture enables the service provider to build the MPLS VPN network one time and add VPNs for new customers as needed, including them in the already established network. The elements that comprise the MPLS VPN are:

- Customer edge (CE) routers--The routers to which subscribers in a customer's network connect. The CE router connects to a service provider's edge router (PE router). The CE router initiates the remote access session to the PE router.
- Provider edge (PE) routers--The routers located at the edge of the service provider's MPLS core network. The PE router connects to one or more CE routers and has full knowledge of the routes to the VPNs associated with those CE routers. The PE router does not have knowledge of the routes to VPNs whose associated CE routers are not connected to it.
- Provider (P) routers--The service provider routers that comprise the provider's core network. The P routers do not assign VPN information and they do not have any knowledge of CE routers. Instead, the main focus of the P router is on label switching.

The figure below shows an example of MPLS VPN network architecture.

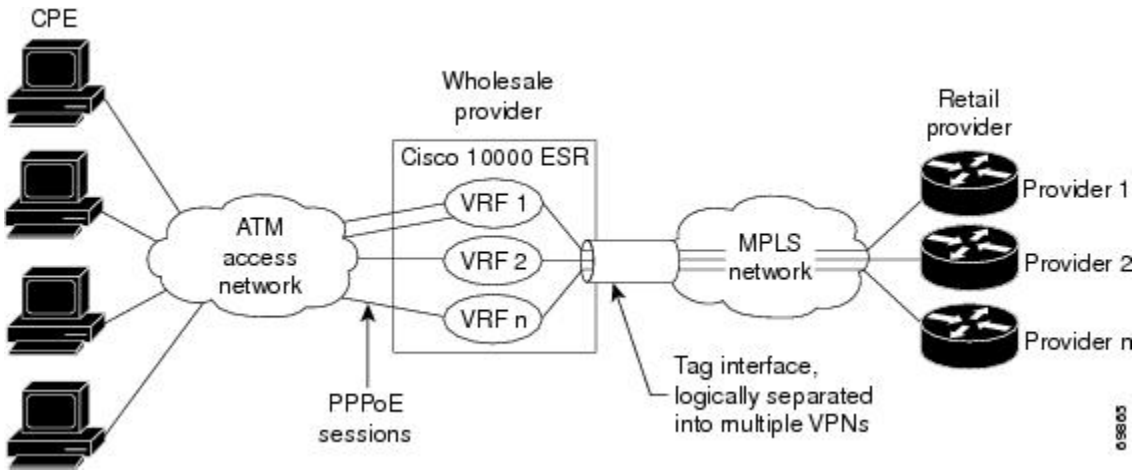
Figure 2 MPLS VPN Network--Example



PPP over Ethernet to MPLS VPN

The figure below shows the topology of integrated PPP over Ethernet (PPPoE) access to an MPLS VPN.

Figure 3 PPPoE Access to MPLS VPN Topology



In the figure above, the service provider operates an MPLS VPN that interconnects all customer sites. The service provider's core network is an MPLS backbone with VPN service capability. The service provider provides all remote access operations to its customer. The network-side interfaces are tagged interfaces, logically separated into multiple VPNs.

Remote access is provided using a PPPoE connection. In this model, when a remote user attempts to establish a connection with a corporate network, a PPPoE session is initiated and is terminated on the

service provider's virtual home gateway (VHG) or PE router. All remote hosts connected to a particular CE router must be part of the VPN to which the CE router is connected.

The PPPoE to MPLS VPN architecture is a flexible architecture with the following characteristics:

- A remote host can create multiple concurrent PPPoE sessions, each to a different VPN.
- If multiple remote hosts exist behind the same CE router, each remote host can log in to a different VPN.
- Any remote host can log in to any VPN at any time because each VHG or PE router has the VRFs for all possible VPNs preinstantiated on it. This configuration requires that the VRF be applied through the RADIUS server, which can cause scalability issues.

The following events occur as the VHG or PE router processes the incoming PPPoE session:

1. A PPPoE session is initiated over the broadband access network.
2. The VHG/PE router accepts and terminates the PPPoE session.
3. The VHG/PE router obtains virtual access interface (VAI) configuration information:
   - The VHG/PE obtains a virtual template interface configuration information, which typically includes VRF mapping for sessions.
   - The VHG/PE sends a separate request to either the customer's or service provider's RADIUS server for the VPN to authenticate the remote user.
   - The VPN's VRF instance is instantiated on the VHG or PE. The VPN's VRF contains a routing table and other information associated with a specific VPN.

Typically, the customer RADIUS server is located within the customer VPN. To ensure that transactions between the VHG/PE router and the customer RADIUS server occur over routes within the customer VPN, the VHG/PE router is assigned at least one IP address that is valid within the VPN.

1. The VHG/PE router forwards accounting records to the service provider's proxy RADIUS server, which in turn logs the accounting records and forwards them to the appropriate customer RADIUS server.
2. The VHG/PE obtains an IP address for the CPE. The address is allocated from one of the following:
   - Local address pool
   - Service provider's RADIUS server, which either specifies the address pool or directly provides the address
   - Service provider's DHCP server
3. The CPE is now connected to the customer VPN. Packets can flow to and from the remote user.

How to Configure Remote Access MPLS-VPNs

Configuring the MPLS Core Network

The MPLS core network is configured by enabling label switching of IP packets on interfaces, configuring virtual routing and forwarding instances, associating VRFs and configuring Multiprotocol BGP PE-to-PE routing sessions. For details relating to these activities, see the appropriate section of the *Cisco IOS XE Multiprotocol Label Switching Configuration Guide*.

Configuring PPPoE

Configuring a Virtual Template Interface

To create and configure a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, perform the steps in the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip unnumbered ethernet** *number*
5. **ppp authentication chap**
6. **ppp ipcp address required**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**ip unnumbered ethernet** *number* **Example:** `Router(config-if)# ip unnumbered ethernet 1`	Enables IP without assigning a specific IP address on the LAN.

	Command or Action	Purpose
Step 5	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables PPP authentication on the virtual template interface.
Step 6	**ppp ipcp address required** **Example:** `Router(config-if)# ppp ipcp address required`	(Required for legacy dialup and DSL networks.) Prevents a PPP session from being configured with 0.0.0.0 remote ip address.

Configuring PPPoE in a Broadband Aggregation Group

To configure a broadband aggregation (BBA) group for PPPoE and to link it to the appropriate virtual template interface, perform the steps in the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {**name** | **global**}
4. **virtual-template** *template-number*
5. **sessions per-mac limit** *per-mac-limit*
6. **sessions max limit** *global-pppoe-session-limit*
7. **exit**
8. **interface gigabitethernet** *slot/subslot/port.* [*subinterface*]
9. Command or Action
10. **encapsulation dot1q** *vlan-id*
11. **pppoe enable** [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {**name** | **global**} **Example:** `Router(config)# bba-group pppoe bba1`	Configures a BBA group to be used to establish PPPoE sessions and enters BBA configuration mode • The name argument identifies the BBA group. You can have multiple BBA groups. • The global keyword is the default BBA group used when a BBA group name is not specified.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba)# virtual-template 20`	Specifies the virtual template interface to use to clone virtual access interfaces (VAIs).
Step 5	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba)# sessions per-mac limit 32000`	(Optional) Specifies the maximum number of PPP over Ethernet (PPPoE) sessions allowed per MAC address in a PPPoE profile.
Step 6	**sessions max limit** *global-pppoe-session-limit* **Example:** `Router(config-bba)# sessions max limit 32000`	(Optional) Specifies the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold
Step 7	**exit** **Example:** `Router(config-bba)# exit`	Returns to global configuration mode.
Step 8	**interface gigabitethernet** *slot/subslot/port.* [*subinterface*] **Example:** `Router(config)# interface gigabitethernet 2/0/0.2`	Specifies the interface to which you want to attach the BBA group.
Step 9	Command or Action	Purpose

	Command or Action	Purpose
Step 10	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 2`	Creates an 802.1q sub-interface and specifies the VLAN id.
Step 11	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-subif)# pppoe enable group bba1`	Attaches the BBA group to the VLAN.

Configuring and Associating Virtual Private Networks

A Virtual Private Network (VPN) service can be added to your MPLS configuration by configuring VPNs and associating the VPNs with a virtual template interface. For details relating to these activities, see the Configuring MPLS Layer 3 VPNs module.

Configuration Examples for Remote Access MPLS-VPNs

Example Configuring Remote Access MPLS-VPNs with One VRF for PPPoE Sessions

The following example shows how to configure the RA to MPLS VPN feature with one VRF for PPPoE sessions:

```
!
!Enables the AAA access control model.
aaa new-model
!
!Configures AAA accounting.
aaa authentication login default none
aaa authentication enable default none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default local
aaa session-id common
enable password cisco
!
username pppoe password 0 pppoe
username common password 0 common
!
!Creates the common VRF.
ip vrf common
rd 100:1000
route-target export 100:1000
route-target import 100:1000
!
```

```
!Specifies the BBA group to be used to establish PPPoE sessions and specifies the maximum
!number of PPPoE sessions to be established over a vlan.
bba-group pppoe
virtual-template 1
sessions per-mac limit 32000
!
no virtual-template snmp
!
!Configures the small buffer.
buffers small permanent 15000
!
!Defines the general loopback interface used for reachability to the router and as a
!source IP address for sessions (IBGP, TDP, and so on).
interface Loopback0
ip address 10.16.3.1 255.255.255.255
ip ospf network point-to-point
!
!Creates a loopback interface in the vpn1 VRF. You do this for each customer VRF you IP
!unnumber interfaces to.
interface Loopback1
ip vrf forwarding vpn1
ip address 10.24.1.1 255.255.255.255
!
interface Loopback2
ip vrf forwarding vpn2
ip address 10.8.1.2 255.255.255.255
!
interface gigaethernet 0/0/0
load-interval 30
negotiation auto
no cdp enable
interface gigaethernet 0/0/0.9
encapsulation dot1q 9
pppoe enable
no cdp enable
!
!Enables label switching of IP packets on the interface.
interface GigabitEthernet1/0/0
ip address 10.1.10.1 255.255.0.0
no ip redirects
load-interval 30
negotiation auto
tag-switching ip
!
!Defines the virtual template and associates the common VRF with it.
interface Virtual-Template1
ip vrf forwarding common
ip unnumbered Loopback1
peer default ip address pool common
ppp authentication chap
!
!Configures OSPF to advertise the networks.
router ospf 100
log-adjacency-changes
auto-cost reference-bandwidth 1000
network 10.16.3.1 0.0.0.0 area 0
network 10.1.0.0 0.0.255.255 area 0
!
router rip
version 2
!
!Enters address family configuration mode to configure the VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
version 2
network 10.0.0.0
no auto-summary
exit-address-family
!
!Configures BGP to advertise the networks for the VPN.
router bgp 100
no synchronization
no bgp default ipv4-unicast
```

```
bgp log-neighbor-changes
neighbor 172.16.1.4 remote-as 100
neighbor 172.16.1.4 activate
!
!Enters address family configuration mode to configure the common VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
no auto-summary
no synchronization
aggregate-address 10.10.0.0 255.255.0.0 summary-only
exit-address-family
!
address-family vpnv4
neighbor 172.16.1.4 activate
neighbor 172.16.1.4 send-community both
exit-address-family
!
!Specifies the IP local pool to use for the VRF address assignment.
ip local pool common 10.10.1.1 10.10.126.0
ip classless
!Enters routing information in the routing table for the VRF.
ip route 10.0.0.0 255.0.0.0 FastEthernet0/0/0 10.9.0.1
ip route vrf common 10.22.0.0 255.255.0.0 Null0
ip route vrf common 10.30.0.0 255.255.0.0 2.1.1.1 3
ip route vrf common 10.32.0.0 255.255.0.0 2.2.151.1 2
ip route vrf common 10.33.0.0 255.255.0.0 2.3.101.1 2
no ip http server
ip pim bidir-enable
!
no cdp run
!
!Specifies the RADIUS host and configures RADIUS accounting. radius-server retransmit is
!on by default and cannot be removed.
radius-server host 10.19.100.150 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key test
radius-server authorization permit missing Service-Type
radius-server vsa send authentication
call admission limit 90
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Description of commands associated with MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Command Reference*
Basic MPLS VPNs	Configuring MPLS Layer 3 VPNs

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco 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 Remote Access MPLS-VPNs

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 3 Feature Information for Remote Access MPLS-VPNs

Feature Name	Releases	Feature Information
Remote Access MPLS-VPNs	Cisco IOS XE Release 2.1	The Remote Access MPLS-VPNs feature allows the service provider to offer a scalable end-to-end VPN service to remote users. This feature integrates the MPLS-enabled backbone with broadband access capabilities. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

CE --customer edge.

PPPoE --Point-to-Point Protocol over Ethernet.

PE --provider edge.

MPLS Multi-VRF (VRF-Lite)

The MPLS Multi-VRF feature allows you to configure and maintain more than one instance of a routing and forwarding table within the same customer edge (CE) router.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MPLS Multi-VRF

The network's core and provider edge routers must be configured for MPLS Virtual Private Network (VPN) operation.

Restrictions for MPLS Multi-VRF

You can configure the MPLS Multi-VRF feature only on Layer 3 interfaces.

The MPLS Multi-VRF feature is not supported by Interior Gateway Routing Protocol (IGRP) nor IS-IS.

Label distribution for a given VPN routing and forwarding (VRF) instance on a given router can be handled by either Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP), but not by both protocols at the same time.

Multicast cannot operate on a Layer 3 interface that is configured with the MPLS Multi-VRF feature.

Multicast cannot be configured at the same time on the same layer 3 interface as the MPLS Multi-VRF feature.

Information About MPLS Multi-VRF

How the MPLS Multi-VRF Feature Works

The MPLS Multi-VRF feature enables a service provider to support two or more VPNs, where the IP addresses can overlap several VPNs. The MPLS Multi-VRF feature uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as FastEthernet ports, or logical, such as VLAN Switched Virtual Interfaces (SVIs), but a Layer 3 interface cannot belong to more than one VRF at any one time. The Multi-VRF feature allows an operator to support two or more routing domains on a CE router, with each routing domain having its own set of interfaces and its own set of routing and forwarding tables. The MPLS Multi-VRF feature makes it possible to extend the Label Switched Paths (LSPs) to the CE and into each routing domain that the CE supports.

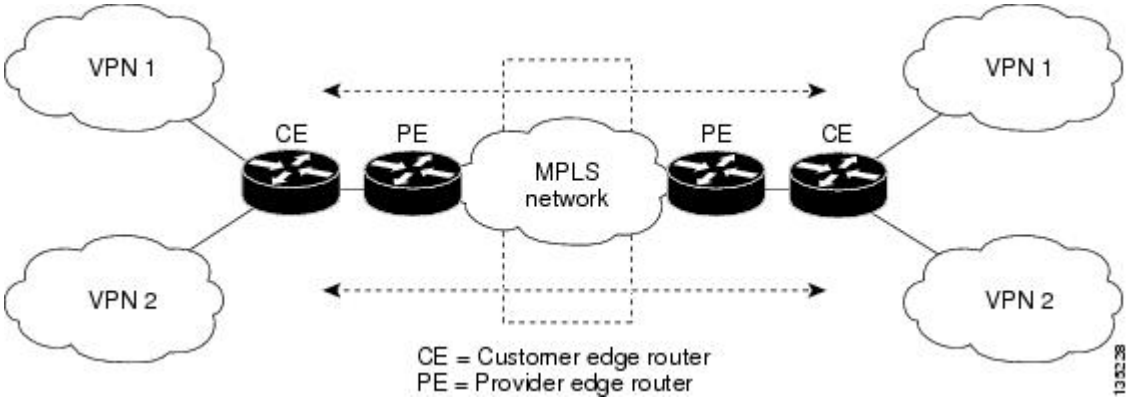
The MPLS Multi-VRF feature works as follows:

- Each CE router advertises its site's local routes to a provider edge (PE) router and learns the remote VPN routes from that PE router.
- PE routers exchange routing information with CE routers by using static routing or a routing protocol such as BGP, RIPv1, or RIPv2.
- PE routers exchange MPLS label information with CE routers through LDP or BGP.
- The PE router needs to maintain VPN routes only for those VPNs to which it is directly attached, eliminating the requirement that the PE maintain all of the service provider's VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Two or more interfaces on a PE router can be associated with a single VRF if all the sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CE routers, the PE router exchanges VPN routing information with other PE routers through internal BGP (iBPG).

With the MPLS Multi-VRF feature, two or more customers can share one CE router, and only one physical link is used between the CE and the PE routers. The shared CE router maintains separate VRF tables for each customer and routes packets for each customer based on that customer's own routing table. The MPLS Multi-VRF feature extends limited PE router functionality to a CE router, giving it the ability, through the maintenance of separate VRF tables, to extend the privacy and security of a VPN to the branch office.

The figure below shows a configuration where each CE router acts as if it were two CE routers. Because the MPLS Multi-VRF feature is a Layer 3 feature, each interface associated with a VRF must be a Layer 3 interface.

Figure 4 Each CE Router Acting as Several Virtual CE Routers



How Packets Are Forwarded in a Network Using the MPLS Multi-VRF Feature

Following is the packet-forwarding process in an MPLS Multi-VRF CE-enabled network, as illustrated in the figure above :

- When the CE receives a packet from a VPN, it looks up the routing table based on the input interface. When a route is found, the CE imposes the MPLS label it received from the PE for that route and forwards the packet to the PE.
- When the ingress PE receives a packet from the CE, it swaps the incoming label with the corresponding label stack and sends it to the MPLS network.
- When an egress PE receives a packet from the network, it swaps the VPN label with the label it earlier had received for the route from the CE, and forwards it to the CE.
- When a CE receives a packet from an egress PE, it uses the incoming label on the packet to forward the packet to the correct VPN.

To configure Multi-VRF, you create a VRF table and then specify the Layer 3 interface associated with that VRF. Next, you configure the routing protocols within the VPN, and between the CE and the PE. BGP is the preferred routing protocol for distributing VPN routing information across the provider's backbone. For more information, see the How to Configure MPLS Multi-VRF, page 62 .

The Multi-VRF network has three major components:

- VPN route target communities: These are lists of all other members of a VPN community. You need to configure VPN route targets for each VPN community member.
- Multiprotocol BGP peering of VPN community PE routers: This propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.
- VPN forwarding: This transports all traffic between VPN community members across a VPN service-provider network.

Points to Consider When Configuring the MPLS Multi-VRF Feature

Consider these points when configuring the MPLS Multi-VRF feature in your network:

- A router with the MPLS Multi-VRF feature is shared by several customers, and each customer has its own routing table.
- Because each customer uses a different VRF table, the same IP addresses can be reused. Overlapping IP addresses are allowed in different VPNs.
- The MPLS Multi-VRF feature lets several customers share the same physical link between the PE and the CE routers. Trunk ports with several VLANs separate packets among the customers. Each customer has its own VLAN.
- For the PE router, there is no difference between using the MPLS Multi-VRF feature or using several CE routers.
- The MPLS Multi-VRF feature does not affect the packet switching rate.

How to Configure MPLS Multi-VRF

Configuring VRFs

To configure VRFs, complete the following procedure. Be sure to configure VRFs on both the PE and the CE routers.

If a VRF has not been configured, the router has the following default configuration:

- No VRFs have been defined.
- No import maps, export maps, or route maps have been defined.
- No VRF maximum routes exist.
- Only the global routing table exists on the interface.

Note Multicast cannot be configured at the same time on the same Layer 3 interface as the MPLS Multi-VRF feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **route-target** {**export** | **import** | **both**} *route-target-ext-community*
7. **import map** *route-map*
8. **exit**
9. **interface** *type slot/subslot/port*[**.***subinterface*]
10. **ip vrf forwarding** *vrf-name*
11. **end**
12. **show ip vrf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip routing** **Example:** `Router(config)# ip routing`	Enables IP routing.
Step 4	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf v1`	Names the VRF, and enters VRF configuration mode.

	Command or Action	Purpose
Step 5	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates a VRF table by specifying a route distinguisher. Enter either an autonomous system number and an arbitrary number (xxx:y), or an IP address and an arbitrary number (A.B.C.D:y).
Step 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf)# route-target export 100:1`	Creates a list of import, export, or import and export route target communities for the specified VRF. Enter either an autonomous system number and an arbitrary number (xxx:y), or an IP address and an arbitrary number (A.B.C.D:y). **Note** This command works only if BGP is running.
Step 7	**import map** *route-map* **Example:** `Router(config-vrf)# import map importmap1`	(Optional) Associates a route map with the VRF.
Step 8	**exit** **Example:** `Router(config-vrf)# exit`	Returns to global configuration mode.
Step 9	**interface** *type slot*/*subslot*/*port*[**.***subinterface*] **Example:** `Router(config)# interface fastethernet3/0/0.10`	Specifies the Layer 3 interface to be associated with the VRF and enters interface configuration mode. The interface can be a routed port or an SVI.
Step 10	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding v1`	Associates the VRF with the Layer 3 interface.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 12	**show ip vrf** **Example:** `Router# show ip vrf`	Displays the settings of the VRFs.

Configuring BGP as the Routing Protocol

Most routing protocols can be used between the CE and the PE routers. However, external BGP (eBGP) is recommended, because:

- ◦ BGP does not require more than one algorithm to communicate with many CE routers.
  ◦ BGP is designed to pass routing information between systems run by different administrations.
  ◦ BGP makes it easy to pass attributes of the routes to the CE router.

When BGP is used as the routing protocol, it can also be used to handle the MPLS label exchange between the PE and CE routers. By contrast, if OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

To configure a BGP PE-to-CE routing session, perform the following steps on the CE and on the PE routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *ip-address* **mask** *network-mask*
5. **redistribute ospf** *process-id* **match internal**
6. **network** *ip-address* **area** *area-id*
7. **address-family ipv4 vrf** *vrf-name*
8. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
9. **neighbor** *address* **activate**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Command or Action	Purpose
Step 2 **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3 **router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 100`	Configures the BGP routing process with the autonomous system number passed to other BGP routers, and enters router configuration mode.
Step 4 **network** *ip-address* **mask** *network-mask* **Example:** `Router(config-router)# network 10.0.0.0 mask 255.255.255.0`	Specifies a network and mask to announce using BGP.
Step 5 **redistribute ospf** *process-id* **match internal** **Example:** `Router(config-router)# redistribute ospf 2 match internal`	Sets the router to redistribute OSPF internal routes.
Step 6 **network** *ip-address* **area** *area-id* **Example:** `Router(config-router)# network 10.0.0.0 255.255.255.0 area 0`	Identifies the network address and mask on which OSPF is running, and the area ID of that network address.
Step 7 **address-family ipv4 vrf** *vrf-name* **Example:** `Router(config-router)# address-family ipv4 vrf v12`	Identifies the name of the VRF instance that will be associated with the next two commands, and enters VRF address-family mode.
Step 8 **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* **Example:** `Router(config-router-af)# neighbor 10.0.0.3 remote-as 100`	Informs this router's BGP neighbor table of the neighbor's address (or peer group name) and the neighbor's autonomous system number.

	Command or Action	Purpose
Step 9	**neighbor** *address* **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.3 activate`	Activates the advertisement of the IPv4 address-family neighbors.

Configuring PE-to-CE MPLS Forwarding and Signalling with BGP

If BGP is used for routing between the PE and the CE routers, configure BGP to signal the labels on the VRF interfaces of both the CE and the PE routers. You must enable signalling globally at the router configuration level and for each interface:

- At the router-configuration level, to enable MPLS label signalling via BGP, use the **neighbor send-label** command).
- At the interface level, to enable MPLS forwarding on the interface used for the PE-to-CE eBGP session, use the **mpls bgp forwarding** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4 vrf** *vrf-name*
5. **neighbor** *address* **send-label**
6. **neighbor** *address* **activate**
7. **end**
8. **configure terminal**
9. **interface** *type slot/subslot/port*[**.***subinterface*]
10. **mpls bgp forwarding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 100`	Configures the BGP routing process with the autonomous system number passed to other BGP routers and enters router configuration mode.
Step 4	**address-family ipv4 vrf** *vrf-name* **Example:** `Router(config-router)# address-family ipv4 vrf v12`	Identifies the name of the VRF instance that will be associated with the next two commands and enters address family configuration mode.
Step 5	**neighbor** *address* **send-label** **Example:** `Router(config-router-af)# neighbor 10.0.0.3 remote-as 100`	Enables the router to use BGP to distribute MPLS labels along with the IPv4 routes to the peer router(s). If a BGP session is running when you issue this command, the command does not take effect until the BGP session is restarted.
Step 6	**neighbor** *address* **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.3 activate`	Activates the advertisement of the IPv4 address-family neighbors.
Step 7	**end** **Example:** `Router(config-router-af)# end`	Returns to privileged EXEC mode.
Step 8	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 9	**interface** *type slot/subslot/port*[**.***subinterface*] **Example:** `Router(config)# interface fastethernet3/0/0.10`	Enters interface configuration mode for the interface to be used for the BGP session. The interface can be a routed port or an SVI.
Step 10	**mpls bgp forwarding** **Example:** `Router(config-if)# mpls bgp forwarding`	Enables MPLS forwarding on the interface.

Configuring a Routing Protocol Other than BGP

You can use RIP, EIGRP, OSPF or with static routing. This configuration uses OSPF, but the process is the same for other protocols.

If you use OSPF as the routing protocol between the PE and the CE routers, issue the **capability vrf-lite** command in router configuration mode. See *OSPF Support for Multi-VRF in CE Routers* for more information.

Note If OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

The MPLS Multi-VRF feature is not supported by IGRP nor IS-IS.

Multicast cannot be configured on the same Layer 3 interface as the MPLS Multi-VRF feature is configured.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **log-adjacency-changes**
5. **redistribute bgp** *autonomous-system-number* **subnets**
6. **network** *ip-address subnet-mask* **area** *area-id*
7. **end**
8. **show ip ospf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 100 vrf v1`	Enables OSPF routing, specifies a VRF table, and enters router configuration mode.
Step 4	**log-adjacency-changes** **Example:** `Router(config-router)# log-adjacency-changes`	(Optional) Logs changes in the adjacency state. This is the default state.
Step 5	**redistribute bgp** *autonomous-system-number* **subnets** **Example:** `Router(config-router)# redistribute bgp 800 subnets`	Sets the router to redistribute information from the BGP network to the OSPF network.
Step 6	**network** *ip-address subnet-mask* **area** *area-id* **Example:** `Router(config-router)# network 10.0.0.0 255.255.255.0 area 0`	Indicates the network address and mask on which OSPF runs, and the area ID of that network address.
Step 7	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	**show ip ospf** **Example:** `Router# show ip ospf`	Displays information about the OSPF routing processes.

Configuring PE-to-CE MPLS Forwarding and Signalling with LDP

SUMMARY STEPS

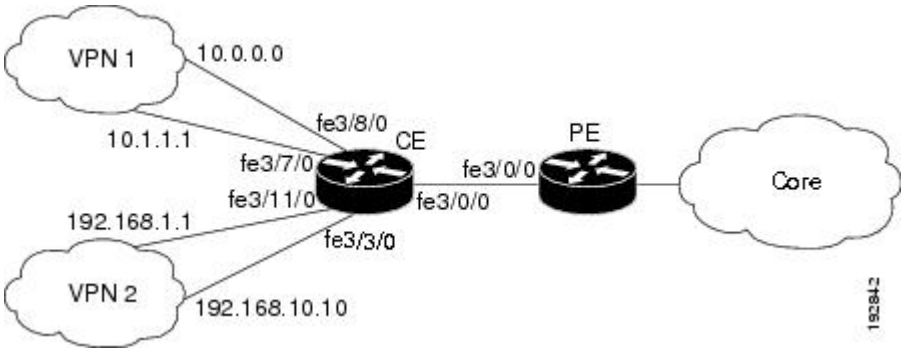
1. **enable**
2. **configure terminal**
3. **interface** *type slot /subslot/port*[**.***subinterface*]
4. **mpls ip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot /subslot/port*[**.***subinterface*] **Example:** `Router(config)# interface fastethernet3/0/0.10`	Enters interface configuration mode for the interface associated with the VRF. The interface can be a routed port or an SVI.
Step 4	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IPv4 packets along normally routed paths for this interface.

Configuration Examples for MPLS Multi-VRF

The figure below is an example of an MPLS Multi-VRF topology.



- Example Configuring MPLS Multi-VRF on the PE Router, page 72
- Example Configuring MPLS Multi-VRF on the CE Router, page 73

Example Configuring MPLS Multi-VRF on the PE Router

Configuring VRFs

```
configure terminal
ip vrf v1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 exit
ip vrf v2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 exit
```

Configuring PE-to-CE Connections Using BGP for Both Routing and Label Exchange

```
router bgp 100
 address-family ipv4 vrf v2
  neighbor 10.0.0.8 remote-as 800
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-label
  exit
 address-family ipv4 vrf vl
  neighbor 10.0.0.8 remote-as 800
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-label
  end
configure terminal
 interface fastethernet3/0/0.10
  ip vrf forwarding v1
  ip address 10.0.0.3 255.255.255.0
  mpls bgp forwarding
  exit
 interface fastethernet3/0/0.20
  ip vrf forwarding v2
  ip address 10.0.0.3 255.255.255.0
```

```
 mpls bgp forwarding
 exit
```

Configuring PE-to-CE Connections Using OSPF for Routing and LDP for Label Exchange

```
router ospf 100 vrf v1
 network 10.0.0.0 255.255.255.0 area 0
 exit
router ospf 101 vrf v2
 network 10.0.0.0 255.255.255.0 area 0
 exit
interface fastethernet3/0/0.10
 ip vrf forwarding v1
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
interface fastethernet3/0/0.20
 ip vrf forwarding v2
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
```

Example Configuring MPLS Multi-VRF on the CE Router

Configuring VRFs

```
configure terminal
 ip routing
 ip vrf v11
  rd 800:1
  route-target export 800:1
  route-target import 800:1
  exit
 ip vrf v12
  rd 800:2
  route-target export 800:2
  route-target import 800:2
  exit
```

Configuring CE Router VPN Connections

```
interface fastethernet3/8/0
ip vrf forwarding v11
ip address 10.0.0.8 255.255.255.0
exit
interface fastethernet3/11/0
ip vrf forwarding v12
ip address 10.0.0.8 255.255.255.0
exit
  router ospf 1 vrf v11
 network 10.0.0.0 255.255.255.0 area 0
 network 10.0.0.0 255.255.255.0 area 0
 exit
  router ospf 2 vrf v12
 network 10.0.0.0 255.255.255.0 area 0
 network 10.0.0.0 255.255.255.0 area 0
 exit
```

Note If BGP is used for routing between the PE and CE routers, the BGP-learned routes from the PE router can be redistributed into OSPF using the commands in the following example.

```
 router ospf 1 vrf v11
```

```
redistribute bgp 800 subnets
exit
 router ospf 2 vrf v12
redistribute bgp 800 subnets
exit
```

Configuring PE-to-CE Connections Using BGP for Both Routing and Label Exchange

```
 router bgp 800
address-family ipv4 vrf v12
neighbor 10.0.0.3 remote-as 100
neighbor 10.0.0.3 activate
neighbor 10.0.0.3 send-label
redistribute ospf 2 match internal
exit
address-family ipv4 vrf vl1
neighbor 10.0.0.3 remote-as 100
neighbor 10.0.0.3 activate
neighbor 10.0.0.3 send-label
redistribute ospf 1 match internal
end
 interface fastethernet3/0/0.10
 ip vrf forwarding v11
 ip address 10.0.0.8 255.255.255.0
 mpls bgp forwarding
 exit
 interface fastethernet3/0/0.20
 ip vrf forwarding v12
 ip address 10.0.0.8 255.255.255.0
 mpls bgp forwarding
 exit
```

Configuring PE-to-CE Connections Using OSPF for Routing and LDP for Label Exchange

```
 router ospf 1 vrf v11
network 10.0.0.0 255.255.255.0 area 0
exit
 router ospf 2 vrf v12
network 10.0.0.0 255.255.255.0 area 0
exit
 interface fastethernet3/0/0.10
 ip vrf forwarding v11
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
 interface fastethernet3/0/0.20
 ip vrf forwarding v12
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Description of commands associated with MPLS and MPLS application	*Cisco IOS Multiprotocol Label Switching Command Reference*

Related Topic	Document Title
OSPF with Multi-VRF	*OSPF Support for Multi-VRF in CE Routers*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco 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 Multi-VRF

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 4 Feature Information for MPLS Multi-VRF

Feature Name	Releases	Feature Information
MPLS Multi-VRF	Cisco IOS XE Release 2.1	The MPLS Multi-VRF feature allows you to configure and maintain more than one instance of a routing and forwarding table within the same CE router.

Multi-VRF Selection Using Policy-Based Routing

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature allows a specified interface on a provider edge (PE) router to route packets to Virtual Private Networks (VPNs) based on packet length or match criteria defined in an IP access list.

You can enable VPN routing and forwarding (VRF) selection by policy routing packets through a route map, through the global routing table, or to a specified VRF.

You can enable policy-routing packets for VRF instances by using route map commands with **set** commands.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Multi-VRF Selection Using Policy-Based Routing

- The router must support policy-based routing (PBR) in order for you to configure this feature.

- A VRF must be defined before you configure this feature. An error message is displayed on the console if no VRF exists.

Restrictions for Multi-VRF Selection Using Policy-Based Routing

- All commands that aid in routing also support hardware switching, except for the **set ip next-hop verify availability** command because Cisco Discovery Protocol information is not available in the line cards.
- Protocol Independent Multicast (PIM) and multicast packets do not support PBR and cannot be configured for a source IP address that is a match criterion for this feature.
- The **set vrf** and **set ip global next-hop** commands can be configured with the **set default interface**, **set interface** , **set ip default next-hop**, and **set ip next-hop** commands. But the **set vrf** and **set ip global next-hop** commands take precedence over the **set default interface**, **set interface** , **set ip default next-hop**, and **set ip next-hop** commands. No error message is displayed if you attempt to configure the **set vrf** command with any of these three **set** commands.
- The Multi-VRF Selection Using Policy-Based Routing (PBR) feature cannot be configured with IP prefix lists.
- The **set global** and **set vrf** commands cannot be simultaneously applied to a route map.
- The Multi-VRF Selection Using Policy-Based Routing (PBR) feature supports VRF-lite; that is, only IP routing protocols run on the router. Multiprotocol Label Switching (MPLS) and VPN cannot be configured.

Information About Multi-VRF Selection Using Policy-Based Routing

Policy Routing of VPN Traffic Based on Match Criteria

The Multi-VRF Selection Using Policy-Based Routing feature is an extension of the VRF Selection Based on Source IP Address feature. The PBR implementation of the VRF selection feature allows you to policy route VPN traffic based on match criteria. Match criteria are defined in an IP access list and/or are based on packet length. The following match criteria are supported in Ciscosoftware:

- IP access lists—Define match criteria based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access list configuration options in Cisco software can be used to define match criteria.
- Packet lengths—Define match criteria based on the length of a packet, in bytes. The packet length filter is defined in a route map with the **match length** route-map configuration command.

Policy routing is defined in the route map. The route map is applied to the incoming interface with the **ip policy route-map** interface configuration command. An IP access list is applied to the route map with the **match ip address** route-map configuration command. Packet length match criteria are applied to the route

map with the **match length** route-map configuration command. The **set** action is defined with the **set vrf** route-map configuration command. The match criteria are evaluated, and the appropriate VRF is selected by the **set** command. This combination allows you to define match criteria for incoming VPN traffic and policy route VPN packets out to the appropriate VRF.

Policy-Based Routing set Commands

Policy-routing Packets for VRF Instances

To enable policy-routing packets for VRF instances, you can use route map commands with the following **set** commands. They are listed in the order in which the router uses them during the routing of packets.

- **set TOS**—Sets the Type of Service (TOS) bits in the header of an IP packet.
- **set DF**—Sets the Don't Fragment (DF) bit in the header of an IP packet.
- **set vrf**—Routes packets through the specified interface. The interface can belong to the global routing table or to any other VRF instance.
- **set global**—Routes packets through the global routing table. This command is useful for routing ingress packets belonging to a specific VRF through the global routing table.
- **set ip vrf next-hop**—Indicates where to output packets that pass a match criteria of a route map for policy routing when the next hop must be under a specified VRF.
- **set ip global next-hop**—Indicates where to forward packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS XE software uses the global routing table.
- **set interface**—When packets enter a VRF, routes the packets out of the egress interface under the same VRF according to the set interface policy, provided that the Layer 2 rewrite information is available.
- **set ip default vrf**—Provides inherit-VRF and inter-VRF routing. With inherit-VRF routing, packets arriving at a VRF interface are routed by the same outgoing VRF interface. With inter-VRF routing, packets arriving at a VRF interface are routed via any other outgoing VRF interface.
- **set ip default global**—Provides VRF to global routing.
- **set default interface**—Indicates where to output packets that pass a match criterion of a route map for policy routing and have no explicit route to the destination. The interface can belong to any VRF.
- **set ip global next-hop**—Routes packets through the global routing table, where the next hop lookup will be in the global routing table.
- **set ip default next-hop**—Indicates where to output packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS XE software has no explicit route to a destination.
- **set ip precedence**—Sets the IP precedence bit in the header of an IP packet.

Change of Normal Routing and Forwarding Behavior

When you configure PBR, you can use the following four **set** commands to change normal routing and forwarding behavior. Configuring any of these **set** commands overrides the routing behavior of packets entering the interface if the packets do not belong to a VRF. The packets are routed from the egress interface across the global routing table.

- **set default interface**—Indicates where to output packets that pass a match criterion of a route map for policy routing and have no explicit route to the destination.
- **set interface**—When packets enter a VRF, routes the packets out of the egress interface under the same VRF according to the set interface policy, provided that the Layer 2 rewrite information is available.

Note The interface must be a peer-to-peer (P2P) interface.

- **set ip default next-hop**—Indicates where to output packets that pass a match criterion of a route map for policy routing and for which the Cisco IOS XE software has no explicit route to a destination.
- **set ip next-hop**—Indicates where to output packets that pass a match criterion of a route map for policy routing.

Support of Inherit-VRF Inter-VRF and VRF-to-Global Routing

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature supports inherit-VRF and inter-VRF. With inherit-VRF routing, packets arriving at a VRF interface are routed by the same outgoing VRF interface. With inter-VRF routing, packets arriving at a VRF interface are routed via any other outgoing VRF interface.

VRF-to-global routing causes packets that enter any VRF interface to be routed via the global routing table. When a packet arrives on a VRF interface, the destination lookup normally is done only in the corresponding VRF table. If a packet arrives on a global interface, the destination lookup is done in the global routing table.

The Multi-VRF Selection Using Policy-Based Routing (PBR) feature modifies the following **set** commands to support inherit-VRF, inter-VRF, and VRF-to-global routing. The commands are listed in the order in which the router uses them during the routing of packets.

- **set global**—Routes packets through the global routing table. This command is useful for routing ingress packets belonging to a specific VRF through the global routing table.
- **set ip global next-hop**—Indicates where to forward packets that pass a match criterion of a route map for policy routing and for which the Cisco software uses the global routing table.
- **set ip vrf next-hop**—Causes the router to look up the next hop in the VRF table. If a packet arrives on an interface that belongs to a VRF and the packet needs to be routed via a different VRF, you can use the **set ip vrf next-hop** command.
- **set ip default vrf**—Provides inherit-VRF and inter-VRF routing. With inherit-VRF routing, packets arriving at a VRF interface are routed by the same outgoing VRF interface. With inter-VRF routing, packets arriving at a VRF interface are routed via any other outgoing VRF interface.
- **set interface**—When packets enter a VRF, routes the packets out of the egress interface under the same VRF, according to the set interface policy, provided that the Layer 2 rewrite information is available.
- **set default interface**—Indicates where to output packets that pass a match criterion of a route map for policy routing and have no explicit route to the destination. The interface can belong to any VRF.
- **set ip next-hop**—Routes packets through the global routing table in an IP-to-IP routing and forwarding environment.
- **set vrf**—Selects the appropriate VRF after a successful match occurs in the route map. VRS-aware PSV allows only inter-VRF (or VRF-to-VRF) switching.

How to Configure Multi-VRF Selection Using Policy-Based Routing

Defining the Match Criteria for Multi-VRF Selection Using PBR

Define the match criteria for multi-VRF selection using PBR so that you can selectively route the packets instead of using their default routing and forwarding.

The match criteria for multi-VRF selection using PBR are defined in an access list. Standard, named, and extended access lists are supported.

You can define the match criteria based on the packet length by configuring the **match length** route-map configuration command. This configuration option is defined entirely within a route map.

The following sections explain how to configure PBR route selection:

Configuring Multi-VRF Selection Using PBR with a Standard Access List

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} [**source** *source-wildcard*] [**log**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} [**source** *source-wildcard*] [**log**] **Example:** `Router(config)# access-list 40 permit source 10.1.1.0/24 0.0.0.255`	Creates an access list and defines the match criteria for the route map. • Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. You can use all IP access list configuration options to define match criteria. • The example creates a standard access list numbered 40. This filter permits traffic from any host with an IP address in the 10.1.1.0/24 subnet.

Configuring Multi-VRF Selection Using PBR with a Named Extended Access List

To configure Multi-VRF Selection using PBR with a named extended access list, complete the following steps.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*]
4. [*sequence-number*] {**permit** | **deny**} *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos***tos*] [**ttl** *operator-vaue*] [**log**] [**time-range** *time-range-name*] [**fragments**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*] **Example:** `Router(config)# ip access-list extended NAMEDACL`	Specifies the IP access list type and enters the corresponding access list configuration mode. • You can specify a standard, extended, or named access list.
Step 4	[*sequence-number*] {**permit** | **deny**} *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos***tos*] [**ttl** *operator-vaue*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Router(config-ext-nacl)# permit ip any any option any-options`	Defines the criteria for which the access list will permit or deny packets. • Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. You can use all IP access list configuration options to define match criteria. • The example creates a named access list that permits any configured IP option.

Configuring Multi-VRF Selection in a Route Map

Incoming packets are filtered through the match criteria that are defined in the route map. After a successful match occurs, the **set vrf** command configuration determines the VRF through which the outbound VPN packets will be policy routed.

You must define the VRF before you configure the route map; otherwise an error message appears on the console.

A receive entry must be added to the VRF selection table with the **ip vrf receive** command. If a match and set operation occurs in the route map but there is no receive entry in the local VRF table, the packet will be dropped if the packet destination is local.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. Do one of the following:
   - **set ip vrf** *vrf-name* **next-hop** *ip-address* [*...ip-address*]
   - or
   - **set ip next-hop recursive vrf** *ip-address* [*...ip-address*]
   - or
   - **set ip global next-hop** *ip-address* [*...ip-address*]
5. Do one of the following:
   - **match ip address** {*acl-number* [*acl-name* | *acl-number*]}
   - or
   - **match length** *minimum-lengthmaximum-length*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** `Router(config)# route-map map1 permit 10`	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. • Enters route-map configuration mode.

Command or Action	Purpose

Step 4 Do one of the following:
• **set ip vrf** *vrf-name* **next-hop** *ip-address* [*...ip-address*]
• or
• **set ip next-hop recursive vrf** *ip-address* [*...ip-address*]
• or
• **set ip global next-hop** *ip-address* [*...ip-address*]
Example:
`Router(config-route-map)# set ip vrf myvrf next-hop 10.0.0.0`
Example:
`Router(config-route-map)# set ip next-hop recursive vrf 10.0.0.0`
Example:
`Router(config-route-map)# set ip global next-hop 10.0.0.0`
	Indicates where to forward packets that pass a match criterion of a route map for policy routing when the next hop must be under a specified VRF.
	or
	Indicates which destination or next hop will be used for packets that pass the match criterion configured in the route map.
	or
	Indicates where to forward packets that pass a match criterion of a route map for policy routing and for which the software uses the global routing table.

Step 5 Do one of the following:
• **match ip address** {*acl-number* [*acl-name* | *acl-number*]}
• or
• **match length** *minimum-lengthmaximum-length*
Example:
`Router(config-route-map)# match ip address 1 or`
Example:
`Router(config-route-map)# match length 3 200`
	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on matched packets. IP access lists are supported.
	• The example configures the route map to use standard access list 1 to define match criteria.
	or
	Specifies the Layer 3 packet length in the IP header as a match criterion in a class map.
	• The example configures the route map to match packets that are 3 to 200 bytes in length.

Step 6 **end** **Example:** `Router(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

Configuring Multi-VRF Selection Using PBR and IP VRF Receive on the Interface

The route map is attached to the incoming interface with the **ip policy route-map** interface configuration command.

The source IP address must be added to the VRF selection table. VRF selection is a one-way (unidirectional) feature. It is applied to the incoming interface. If a **match** and **set** operation occurs in the route map but there is no receive entry in the local VRF table, the packet is dropped if the packet destination is local.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip vrf receive** *vrf-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface FastEthernet 0/1/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip policy route-map** *map-tag* **Example:** `Router(config-if)# ip policy route-map map1`	Identifies a route map to use for policy routing on an interface. • The configuration example attaches the route map named map1 to the interface.

	Command or Action	Purpose
Step 5	**ip vrf receive** *vrf-name* **Example:** `Router(config-if)# ip vrf receive VRF-1`	Adds the IP addresses that are associated with an interface into the VRF table. • This command must be configured for each VRF that will be used for VRF selection.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Multi-VRF Selection Using PBR

To verify the configuration of the Multi-VRF Selection Using Policy-Based Routing (PBR) feature, perform the following steps. You can enter the commands in any order.

SUMMARY STEPS

1. **show ip access-list** [*access-list-number* | *access-list-name*]
2. **show route-map** [*map-name*]
3. **show ip policy**

DETAILED STEPS

Step 1 **show ip access-list** [*access-list-number* | *access-list-name*]

To verify the configuration of match criteria for PBR multi-VRF selection, use the **show ip access-list** command. The following **show ip access-list** command output displays three subnet ranges defined as match criteria in three standard access lists:

Example:

```
Router# show ip access-list

Standard IP access list 40
 10 permit 10.1.0.0, wildcard bits 0.0.255.255
Standard IP access list 50
 10 permit 10.2.0.0, wildcard bits 0.0.255.255
Standard IP access list 60
 10 permit 10.3.0.0, wildcard bits 0.0.255.255
```

Step 2 **show route-map** [*map-name*]

Use this command to verify **match** and **set** commands within the route map:

Example:

```
Router# show route-map
```

To verify the route-map configuration, use the **show route-map** command. The output displays the match criteria and set action for each route-map sequence. The output also displays the number of packets and bytes that have been policy routed per each route-map sequence.

Example:

```
Router# show route-map map1
route-map map1, permit, sequence 10
Match clauses:
Set clauses:
 ip next-hop vrf myvrf 10.5.5.5  10.6.6.6  10.7.7.7
 ip next-hop global 10.8.8.8  10.9.9.9
Policy routing matches: 0 packets, 0 bytes
Router# show route-map map2
route-map map2, permit, sequence 10
Match clauses:
Set clauses:
 vrf myvrf
Policy routing matches: 0 packets, 0 bytes
Router# show route-map map3
route-map map3, permit, sequence 10
Match clauses:
Set clauses:
 global
Policy routing matches: 0 packets, 0 bytes
```

The following **show route-map** command displays output from the **set ip vrf next-hop** command:

Example:

```
Router(config)# route-map test

Router(config-route-map)# set ip vrf myvrf next-hop
Router(config-route-map)# set ip vrf myvrf next-hop 192.168.3.2
Router(config-route-map)# match ip address 255 101
Router(config-route-map)# end
Router# show route-map

route-map test, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip vrf myvrf next-hop 192.168.3.2
 Policy routing matches: 0 packets, 0 bytes
```

The following **show route-map** command displays output from the **set ip global** command:

Example:

```
Router(config)# route-map test
Router(config-route-map)# match ip address 255 101
Router(config-route-map)# set ip global next-hop 192.168.4.2
Router(config-route-map)# end
Router# show route-map

*May 25 13:45:55.551: %SYS-5-CONFIG_I: Configured from console by consoleout-map
route-map test, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip global next-hop 192.168.4.2
 Policy routing matches: 0 packets, 0 bytes
```

Step 3 **show ip policy**

To verify the PBR multi-VRF selection policy, use the **show ip policy** command:

Example:

```
Router# show ip policy
```

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

Example:

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

Configuration Examples for Multi-VRF Selection Using Policy-Based Routing

Defining the Match Criteria for Multi-VRF Selection Using PBR Example

In the following example, three standard access lists are created to define match criteria for three different subnetworks. Any packets received on FastEthernet interface 0/1/0 will be policy routed through the PBR-VRF-Selection route map to the VRF that is matched in the same route-map sequence. If the source IP address of the packet is part of the 10.1.0.0/24 subnet, VRF1 will be used for routing and forwarding.

```
access-list 40 permit source 10.1.0.0 0.0.255.255
access-list 50 permit source 10.2.0.0 0.0.255.255
access-list 60 permit source 10.3.0.0 0.0.255.255
route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF1
 !
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF2
 !
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF3
 !
interface FastEthernet 0/1/0
 ip address 192.168.1.6 255.255.255.252
 ip vrf forwarding VRF4
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF1
 ip vrf receive VRF2
 ip vrf receive VRF3
```

Configuring Multi-VRF Selection in a Route Map Example

The following example shows a **set ip vrf next-hop** command that applies policy-based routing to the VRF interface named myvrf and specifies that the IP address of the next hop is 10.0.0.2:

```
Router(config)# route-map map1 permit
Router(config)# set vrf myvrf
Router(config-route-map)# set ip vrf myvrf next-hop 10.0.0.2
Router(config-route-map)# match ip address 101
Router(config-route-map)# end
```

The following example shows a **set ip global** command that specifies that the router should use the next hop address 10.0.0.1 in the global routing table:

```
Router(config-route-map)# set ip global next-hop 10.0.0.1
```

Additional References

Related Documents

Related Topic	Document Title
MPLS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Multiprotocol Label Switching Command Reference*
IP access list commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Feature Information for Multi-VRF Selection Using Policy-Based Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for Multi-VRF Selection Using Policy-Based Routing

Feature Name	Releases	Feature Information
Multi-VRF Selection Using Policy-Based Routing (PBR)	Cisco IOS XE Release 2.2	The Multi-VRF Selection Using Policy-Based Routing (PBR) feature allows a specified interface on a provider edge (PE) router to route packets to VPNs based on packet length or match criteria defined in an IP access list. This feature and the VRF Selection Based on Source IP Address feature can be configured together on the same interface. In Cisco IOS XE Release 2.2, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were modified: **set ip global**, **set ip vrf next-hop**, and **set vrf**.

Glossary

CE router—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

Inherit-VRF routing—Packets arriving at a VRF interface are routed by the same outgoing VRF interface.

Inter-VRF routing—Packets arriving at a VRF interface are routed via any other outgoing VRF interface.

IP —Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

PBR —policy-based routing. PBR allows a user to manually configure how received packets should be routed.

PE router—provider edge router. A router that is part of a service provider's network and that is connected to a CE router. It exchanges routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv1, or RIPv2.

VPN —Virtual Private Network. A collection of sites sharing a common routing table. A VPN provides a secure way for customers to share bandwidth over an ISP backbone network.

VRF —A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

VRF-lite —A feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs.

MPLS VPN VRF Selection Using Policy-Based Routing

The MPLS VPN: VRF Selection Using Policy-Based Routing feature is an extension of the MPLS VPN: VRF Selection Based on Source IP Address feature. This feature introduces a policy-based routing (PBR) mechanism to classify and forward Virtual Private Network (VPN) traffic based on multiple VPN routing and forwarding (VRF) selection match criteria.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VRF Selection Using Policy-Based Routing

The router must support PBR.

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

This document assumes that multiprotocol BGP (mBGP), Multiprotocol Label Switching (MPLS), and Cisco Express Forwarding are enabled in your network.

Restrictions for VRF Selection Using Policy-Based Routing

The VRF Selection Using Policy-Based Routing feature is supported only in service provider (-p-) images.

The VRF Selection Using Policy-Based Routing feature can coexist with the VRF Selection Based on Source IP address feature on the same router, but these features cannot be configured together on the same interface. This is designed behavior to prevent VRF table selection conflicts that could occur if these features were misconfigured together. An error message is displayed on the console if you attempt to configure the ip vrf select source and the ip policy route-map commands on the same interface.

Protocol Independent Multicast (PIM) and multicast packets do not support PBR and cannot be configured for a source IP address that is a match criterion for this feature.

The VRF Selection Using Policy-Based Routing feature cannot be configured with IP prefix lists.

Information About VRF Selection Using Policy-Based Routing

Introduction to VRF Selection Using Policy-Based Routing

The VRF Selection Using Policy-Based Routing feature is an extension of the VRF Selection Based on Source IP Address feature. The PBR implementation of the VRF selection feature allows you to policy route VPN traffic based on match criteria. Match criteria are defined in an IP access list or based on packet length. The following match criteria are supported in Cisco software:

- IP access lists--Define match criteria based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access-list configuration options in Cisco software can be used to define match criteria.
- Packet lengths--Define match criteria based on the length of a packet in bytes. The packet length filter is defined in a route map with the **match length** route-map configuration command.

Policy routing is defined in the route map. The route map is applied to the incoming interface with the **ip policy route-map** interface configuration command. An IP access list is applied to the route map with the **match ip address** route-map configuration command. Packet length match criteria are applied to the route map with the **match length** route-map configuration command. The set action is defined with the **set vrf** route-map configuration command. The match criteria are evaluated, and the appropriate VRF is selected by the set clause. This combination allows you to define match criteria for incoming VPN traffic and policy route VPN packets out to the appropriate VRF.

Policy-Based Routing Set Clauses Overview

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

- set default interface
- set interface
- set ip default next-hop
- set ip next-hop

Configuring any of the set clauses will overwrite normal routing forwarding behavior of a packet.

The VRF Selection Using Policy-Based Routing feature introduces the fifth set clause that can be used to change normal routing and forwarding behavior. The set vrf command is used to select the appropriate VRF after the successful match occurs in the route map.

How to Configure VRF Selection Using Policy-Based Routing

Defining the Match Criteria for PBR VRF Selection Based on Packet Length

The match criteria for PBR VRF route selection are defined in an access list. Standard and named access lists are supported. Match criteria can also be defined based on the packet length using the **match length** route-map configuration command. This configuration option is defined entirely within a route map.

Prerequisites

Before you perform this task, make sure that the VRF and associated IP address are already defined.

Configuring PBR VRF Selection with a Standard Access List

Use the following commands to create a standard access list and define the PBR VRF route selection match criteria in it in order to permit or deny the transmission of VPN traffic data packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source-addr* [*source-wildcard*] [**log**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source-addr* [*source-wildcard*] [**log**] **Example:** `Router(config)# access-list 40 permit 10.1.0.0/24 0.0.0.255`	Creates an access list and defines the match criteria for the route map. • Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access-list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access list configuration options in Cisco software can be used to define match criteria. • The example creates a standard access list numbered 40. This filter will permit traffic from any host with an IP address in the 10.1.0.0/24 subnet.

Configuring PBR VRF Selection with a Named Access List

Use the following commands to define the PBR VRF route selection match criteria in a named access list in order to permit or deny the transmission of VPN traffic data packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*]
4. [*sequence-number*] {**permit** | **deny**} *protocol source-addr source-wildcard destination-addr destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*] **Example:** `Router(config)# ip access-list extended NAMEDACL`	Specifies the IP access list type and enters the corresponding access-list configuration mode. • A standard, extended, or named access list can be used.
Step 4	[*sequence-number*] {**permit** | **deny**} *protocol source-addr source-wildcard destination-addr destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Router(config-ext-nacl)# permit ip any any option any-options`	Defines the criteria for which the access list will permit or deny packets. • Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access-list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access-list configuration options in Cisco software can be used to define match criteria. • The example creates a named access list that permits any configured IP option.

Configuring PBR VRF Selection in a Route Map

Use the following commands to configure the VRF through which the outbound VPN packets will be policy routed in order to permit or deny the transmission of VPN traffic data packets.

Incoming packets are filtered through the match criteria that are defined in the route map. After a successful match occurs, the **set vrf** command configuration determines the VRF through which the outbound VPN packets will be policy routed.

- The VRF must be defined prior to the configuration of the route map; otherwise an error message is displayed on the console.
- A receive entry must be added to the VRF selection table with the **ip vrf receive** command. If a match and set operation occurs in the route map but there is no receive entry in the local VRF table, the packet will be dropped if the packet destination is local.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. Do one of the following:
   - **match ip address** {*acl-number* [*acl-number ...* | *acl-name ...*] | *acl-name* [*acl-name ...* | *acl-number ...*]}
   -
   - **match length** *minimum-length maximum-length*
5. **set vrf** *vrf-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map1 permit 10`	Enters route map configuration mode. Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Step 4	Do one of the following:
	• **match ip address** {*acl-number* [*acl-number ...* | *acl-name ...*] | *acl-name* [*acl-name ...* | *acl-number ...*]}
	•
	• **match length** *minimum-length maximum-length*
	
	Example:
	`Router(config-route-map)# match ip address 1`
	
	Example:
	`Router(config-route-map)# match length 3 200`
		Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on matched packets.
		• IP access lists are supported.
		• The example configures the route map to use standard access list 1 to define match criteria.
		or
		Specifies the Layer 3 packet length in the IP header as a match criterion in a class map.
		• The example configures the route map to match packets that are 3 to 200 bytes in size.

Step 5	**set vrf** *vrf-name* **Example:** `Router(config-route-map)# set vrf map1`	Defines which VRF to route VPN packets that are successfully matched in the same route map sequence for PBR VRF selection. • The example policy routes matched packets out to the VRF named map1.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and enters global configuration mode.

Configuring PBR on the Interface

Use the following commands to filter incoming VPN traffic data packets. Incoming packets are filtered through the match criteria that are defined in the route map.

The route map is applied to the incoming interface. The route map is attached to the incoming interface with the **ip policy route-map** global configuration command.

Note

- The VRF Selection Using Policy-Based Routing feature can coexist with the VRF Selection Based on Source IP address feature on the same router, but the two features cannot be configured together on the same interface. This is designed behavior to prevent VRF table selection conflicts that could occur if these features were misconfigured together. An error message is displayed on the console if you attempt to configure the **ip vrf select source** and the **ip policy route-map** commands on the same interface.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip vrf receive** *vrf-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface FastEthernet 0/1/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip policy route-map** *map-tag* **Example:** `Router(config-if)# ip policy route-map map1`	Identifies a route map to use for policy routing on an interface. • The configuration example attaches the route map named map1 to the interface.
Step 5	**ip vrf receive** *vrf-name* **Example:** `Router(config-if)# ip vrf receive VRF1`	Adds the IP addresses that are associated with an interface into the VRF table. • This command must be configured for each VRF that will be used for VRF selection.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.

Configuring IP VRF Receive on the Interface

Use the following commands to insert the IP address of an interface as a connected route entry in a VRF routing table. This will prevent dropped packets.

The source IP address must be added to the VRF selection table. VRF selection is a one-way (unidirectional) feature. It is applied to the incoming interface. If a match and set operation occurs in the route map but there is no VRF receive entry in the local VRF table, the packet will be dropped if the packet destination is local.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip vrf receive** *vrf-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface FastEthernet 0/1/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip policy route-map** *map-tag* **Example:** `Router(config-if)# ip policy route-map map1`	Identifies a route map to use for policy routing on an interface. • The configuration example attaches the route map named map1 to the interface.
Step 5	**ip vrf receive** *vrf-name* **Example:** `Router(config-if)# ip vrf receive VRF1`	Adds the IP addresses that are associated with an interface into the VRF table. • This command must be configured for each VRF that will be used for VRF selection.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode, and enters privileged EXEC mode.

Verifying the Configuration of the VRF Selection Using Policy-Based Routing

To verify the configuration of the VRF Selection Using Policy-Based Routing feature, perform each of the following steps in this section in the order specified.

SUMMARY STEPS

1. **enable**
2. **show ip access-list** [*access-list-number* | *access-list-name*]
3. **show route-map** [*map-name*]
4. **show ip policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip access-list** [*access-list-number* | *access-list-name*] **Example:** `Router# show ip access-list`	Displays the contents of all current IP access lists. • This command is used to verify the match criteria that are defined in the access list. Both named and numbered access lists are supported.
Step 3	**show route-map** [*map-name*] **Example:** `Router# show route-map`	Displays all route maps configured or only the one specified. • This command is used to verify match and set clauses within the route map.

	Command or Action	Purpose
Step 4	**show ip policy** **Example:** `Router# show ip policy`	Displays the route map used for policy routing. • This command can be used to display the route map and the associated interface.

Configuration Examples for VRF Selection Using Policy-Based Routing

Example Defining PBR VRF Selection in Access List

In the following example, three standard access lists are created to define match criteria for three different subnets. Any packets received on the FastEthernet 0/1/0 interface will be policy routed through the PBR-VRF-Selection route map to the VRF that is matched in the same route map sequence. If the source IP address of the packet is part of the 10.1.0.0/24 subnet, VRF1 will be used for routing and forwarding.

```
access-list 40 permit 10.1.0.0 0.0.255.255
access-list 50 permit 10.2.0.0 0.0.255.255
access-list 60 permit 10.3.0.0 0.0.255.255
route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF1
 !
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF2
 !
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF3
 !
interface FastEthernet0/1/0
 ip address 10.1.0.0/24 255.255.255.252
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF1
 ip vrf receive VRF2
 ip vrf receive VRF3
```

Example Verifying VRF Selection Using Policy-Based Routing

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

Verifying Match Criteria

To verify the configuration of match criteria for PBR VRF selection, use the **show ip access-list** command.

The following **show ip access-list** command output displays three subnet ranges defined as match criteria in three standard access lists:

```
Router# show ip access-list
Standard IP access list 40
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
Standard IP access list 50
    10 permit 10.2.0.0, wildcard bits 0.0.255.255
Standard IP access list 60
    10 permit 10.3.0.0, wildcard bits 0.0.255.255
```

Verifying Route-Map Configuration

To verify route-map configuration, use the **show route-map** command. The output displays the match criteria and set action for each route-map sequence. The output also displays the number of packets and bytes that have been policy routed per each route-map sequence.

```
Router# show route-map
route-map PBR-VRF-Selection, permit, sequence 10
  Match clauses:
    ip address (access-lists): 40
  Set clauses:
    vrf VRF1
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 20
  Match clauses:
    ip address (access-lists): 50
  Set clauses:
    vrf VRF2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 30
  Match clauses:
    ip address (access-lists): 60
  Set clauses:
    vrf VRF3
  Policy routing matches: 0 packets, 0 bytes
```

Verifying PBR VRF Selection Policy

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

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
MPLS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Multiprotocol Label Switching Command Reference*
Route-map configuration commands	*Cisco IOS IP Routing Protocols Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

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 VRF Selection Using Policy-Based Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 Feature Information for VRF Selection Using Policy-Based Routing

Feature Name	Releases	Feature Information
MPLS VPN: VRF Selection Using Policy-Based Routing	Cisco IOS XE Release 2.2	The MPLS VPN: VRF Selection Using Policy-Based Routing feature is an extension of the MPLS VPN: VRF Selection Based on Source IP Address feature. This feature introduces a policy-based routing (PBR) mechanism to classify and forward Virtual Private Network (VPN) traffic based on multiple VPN routing and forwarding (VRF) selection match criteria. In Cisco IOS XE Release 2.2, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **ip vrf receive**, **set vrf**.

Glossary

PBR --policy-based routing.

VPN --Virtual Private Network.

VRF --virtual routing and forwarding.

VRF Aware System Message Logging

The VRF Aware System Message Logging (Syslog) feature allows a router to send system logging (syslog) messages to a syslog server host connected through a Virtual Private Network (VPN) routing and forwarding (VRF) interface.

You can use logging information for network monitoring and troubleshooting. This feature extends this capability to network traffic connected through VRFs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VRF Aware System Message Logging

You must configure a VRF on a routing device and associate the VRF with an interface (see the Associating a VRF with an Interface, page 116) before you can configure the VRF Aware System Message Logging feature.

Restrictions for VRF Aware System Message Logging

You cannot specify a source address for VRF system logging messages. The VRF Aware System Message Logging feature uses the VRF interface address as the source address for all VRF-aware system logging messages.

Information About VRF Aware System Message Logging

VRF Aware System Message Logging Benefit

A VPN routing and VRF instance is an extension of IP routing that provides multiple routing instances. A VRF provides a separate IP routing and forwarding table to each VPN. You must configure a VRF on a routing device before you configure the VRF Aware System Message Logging feature.

After you configure the VRF Aware System Message Logging feature on a routing device, the device can send syslog messages to a syslog host through a VRF interface. Then you can use logging messages to monitor and troubleshoot network traffic connected through a VRF. Without the VRF Aware System Message Logging feature on a routing device, you do not have this benefit; the routing device can send syslog messages to the syslog host only through the global routing table.

You can receive system logging messages through a VRF interface on any router where you can configure a VRF, that is:

- On a provider edge (PE) router that is used with Multiprotocol Label Switching (MPLS) and multiprotocol Border Gateway Protocol (BGP) to provide a Layer 3 MPLS VPN network service.
- On a customer edge (CE) device (switch or router) that is configured for VRF-Lite, which is a VRF implementation without multiprotocol BGP.

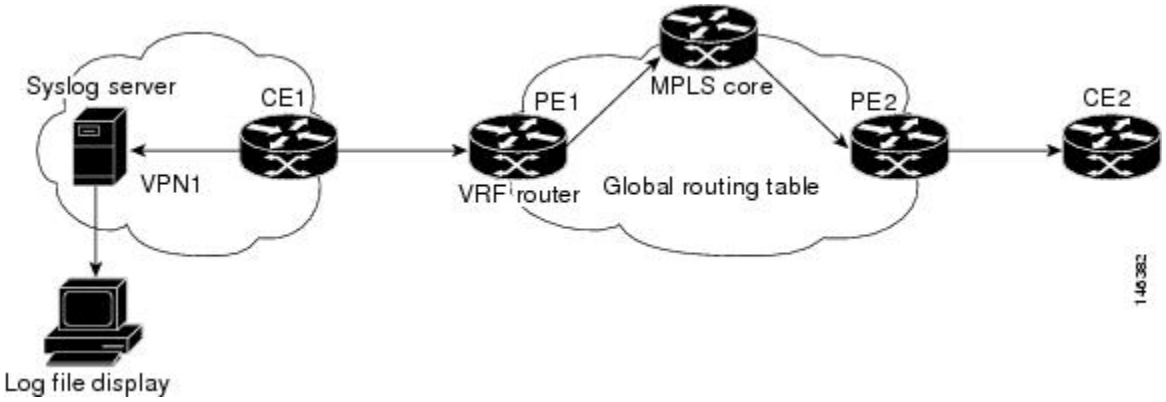
VRF Aware System Message Logging on a Provider Edge Router in an MPLS VPN Network

You can configure the VRF Aware System Message Logging feature on a PE router in a Layer 3 MPLS VPN network. The PE router can then send syslog messages through a VRF interface to a syslog server located in the VPN.

The figure below shows an MPLS VPN network and the VRF Aware System Message Logging feature configured on a PE router associated with VRF VPN1. The PE router sends log messages through a VRF

interface to a syslog server located in VPN1. You can display the messages from the syslog server on a terminal.

Figure 5 MPLS VPN and VRF Aware System Message Logging Configured on a Customer Edge Router

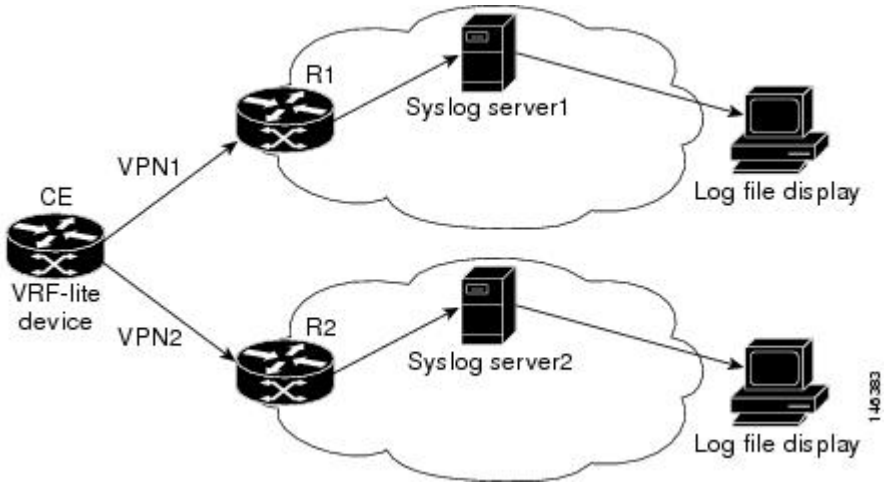


VRF Aware System Message Logging on a Customer Edge Device with VRF-Lite Configured

You can configure the VRF Aware System Message Logging feature on a CE device where you have configured the VRF-Lite feature. The CE device can then send syslog messages through a VRF interface to syslog servers in multiple VPNs. The CE device can be either a router or a switch.

The figure below shows the VRF Aware System Message Logging feature configured on a VRF-Lite CE device. The CE device can send VRF syslog messages to syslog servers in VPN1 or VPN2 or to servers in both VPN1 and VPN2. You can configure multiple VRFs on a VRF-Lite CE device, and the device can serve many customers.

Figure 6 VRF Aware System Message Logging Configured on a VRF-Lite Customer Edge Device



Message Levels for Logging Commands

The table below lists message levels for **logging** commands that you can use when you configure the VRF Aware System Message Logging feature. Information provided by the table below includes keyword level names and numbers, their description, and the associated syslog definitions. You can use either the level keyword name or number with the **logging trap** *level* and **logging buffered** *severity-level* commands.

Table 7 Message Levels for logging Commands

Level Name	Level Number	Description	Syslog Definition
emergencies	**0**	System unusable	LOG_EMERG
alerts	**1**	Immediate action needed	LOG_ALERT
critical	**2**	Critical conditions	LOG_CRIT
errors	**3**	Error conditions	LOG_ERR
warnings	**4**	Warning conditions	LOG_WARNING
notifications	**5**	Normal but significant condition	LOG_NOTICE
informational	**6**	Informational messages only	LOG_INFO
debugging	**7**	Debugging messages	LOG_DEBUG

How to Configure and Verify VRF Aware System Message Logging

Configuring a VRF on a Routing Device

Configuring a VRF on a routing device helps provides customer connectivity to a VPN. The routing device can be a PE router connected to an MPLS VPN network or a CE (switch or router) that is configured for VRF-Lite.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf vpn1`	Defines a VRF and enters VRF configuration mode. • The *vrf-name*argument is a name assigned to the VRF.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF. • The *route-distinguisher* argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. • The route distinquisher (RD) is either an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. • You can enter an RD in either of these formats: ◦ 16-bit autonomous system number: your 32-bit number For example, 101:3. ◦ 32-bit IP address: your 16-bit number For example, 10.0.0.1:1.

	Command or Action	Purpose
Step 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf)# route-target both 100:1`	Creates a route-target extended community for a VRF. • The **import** keyword imports routing information from the target VPN extended community. • The **export** keyword exports routing information to the target VPN extended community. • The **both** keyword imports routing information from and exports routing information to the target VPN extended community. • The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities. The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats: • 16-bit autonomous system 1 32-bit number For example, 101:3. • 32-bit IP address: your 16-bit number For example, 10.0.0.2.15: 1.
Step 6	**end** **Example:** `Router(config-vrf)# end`	Exits to privileged EXEC mode.

Associating a VRF with an Interface

Perform this task to associate a VRF instance with an interface. A VRF must be associated with an interface before you can forward VPN traffic.

Note You cannot configure a source address for VRF system logging messages. The VRF Aware System Message Logging feature uses the VRF interface address as the source address for all VRF-aware system logging messages.

After configuring the VRF and associating it with an interface, you can configure the VRF Aware System Message Logging feature on the routing device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0/0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when the port, connector, or interface card is added to a system, and can be displayed with the **show interfaces** command.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding vpn1`	Associates a VRF with an interface or subinterface. • The *vrf-name* argument associates the interface with the specified VRF.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves configuration changes to NVRAM.

Configuring VRF Aware System Message Logging on a Routing Device

Configure the VRF Aware System Message Logging feature on a routing device so that logging messages can be used to monitor and troubleshoot network traffic connected through VRF instances.

You must perform the following tasks before you perform this task:

- Configure a VRF on a routing device.
- Associate a VRF with an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging host** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
4. **logging trap** *level*
5. **logging facility** *facility-type*
6. **logging buffered** [*buffer-size* | *severity-level*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging host** {*ip-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `Router(config)# logging host 10.0.150.63 vrf vpn1`	Specifies a host to receive syslog messages. • The *ip-address* argument is the IP address of the syslog server host. • The *hostname* argument is the name of the IP or IPv6 host that receives the syslog messages. • The **vrf** *vrf-name* keyword argument pair specifies a VRF that connects to the syslog server host.
Step 4	**logging trap** *level* **Example:** `Router(config)# logging trap debugging`	Limits messages logged to the syslog servers based on severity. • The *level* argument limits the logging of messages to the syslog servers to a specified level. You can enter the level number or level name. See the "Message Levels for Logging Commands" section for a description of acceptable keywords.

	Command or Action	Purpose
Step 5	**logging facility** *facility-type* **Example:** `Router(config)# logging facility local6`	(Optional) Configures the syslog facility in which error messages are sent. • The *facility-type* argument names the syslog facility type keyword. For locally defined messages, the range of acceptable keywords is local0 to local7. The default is **local7**.
Step 6	**logging buffered** [*buffer-size* | *severity-level*] **Example:** `Router(config)# logging buffered debugging`	(Optional) Limits messages logged to an internal buffer on the router based on severity. • The*buffer-size* argument is the size of the buffer from 4096 to 4,294,967,295 bytes. The default size varies by platform. • The *severity-level* argument limits the logging of messages to the buffer to a specified level. You can enter the level name or level number. See the "Message Levels for Logging Commands" section for a list of the acceptable level name or level number keywords. The default logging level varies by platform, but is generally 7, meaning that messages at all levels (0–7) are logged to the buffer.
Step 7	**end** **Example:** `Router(config)# end`	(Optional) Exits to privileged EXEC mode.

Verifying VRF Aware System Message Logging Operation

SUMMARY STEPS

1. **enable**
2. **show running-config | include logging**
3. **show ip vrf interfaces**
4. **show running-config** [**interface** *type number*]
5. **ping vrf** *vrf-name target-ip-address*
6. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show running-config | include logging**

Use this command to display the logging configuration for the router and the logging host for a VRF. For example:

Example:

```
Router# show running-config | include logging
logging queue-limit 100
logging buffered 100000 debugging
mpls ldp logging neighbor-changes
logging trap debugging
logging facility local6
logging host vrf vpn1 10.0.0.3
Router#
```

This example shows the configuration of a syslog server in VRF vpn1 with a server host address of 10.0.0.3.

Step 3 **show ip vrf interfaces**

Use this command to display the interfaces associated with the VRF that links to a syslog server host. The following example displays a list of VRF interfaces and their associated IP addresses that are configured on the router:

Example:

```
Router# show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
FastEthernet0/0/0      10.0.0.0        vpn1                              up
Loopback1              10.0.0.6        vpn1                              up
```

Step 4 **show running-config** [**interface** *type number*]

Use this command to display interface specific configuration information for an interface associated with a VRF. For example:

Example:

```
Router# show running-config interface FastEthernet 0/0/0
Building configuration...
Router#
.
.
.
!
Current configuration : 116 bytes
!
interface FastEthernet0/0/0
 ip vrf forwarding vpn1
 ip address 10.0.0.98 255.0.0.0
 duplex half
 no cdp enable
end
```

This example displays configuration information for Fast Ethernet interface 0/0/0 in VRF vpn1.

Step 5 **ping vrf** *vrf-name target-ip-address*

Use this command to verify that you can reach the syslog server host, the *target-ip-address*, through the specified VRF. For example:

Example:

```
Router# ping vrf vpn1 10.3.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

In this example, the syslog server has an IP address of 10.3.0.1 and the VRF is named vpn1. The server is reached successfully four of five times.

Step 6 **exit**

Use this command to exit privileged EXEC mode. For example:

Example:

```
Router# exit
Router>
```

Configuration Examples for VRF Aware System Message Logging

Example Configuring a VRF on a Routing Device

```
enable
configure terminal
!
ip vrf vpn1
 rd 100:1
 route-target both 100:1
 end
```

Example Associating a VRF with an Interface

```
enable
configure terminal
!
interface FastEthernet 0/0/0
 ip vrf forwarding vpn1
 end
```

Example Configuring VRF Aware System Message Logging on a Routing Device

The following example shows how to configure the VRF Aware System Message Logging feature on a routing device. The IP address of the syslog server host is 10.0.1.3 and the VRF is vpn1.

```
enable
configure terminal
!
 logging host 10.0.1.3 vrf vpn1
 logging trap debugging
 logging facility local6
 logging buffered 10000
 logging buffered debugging
 end
```

The following example shows how to turn off logging to the syslog server:

```
enable
configure terminal
!
 no logging 10.0.1.3
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Description of commands associated with MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Command Reference*
Concepts and tasks for configuring MPLS VPNs	Configuring MPLS Layer 3 VPNs

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco 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 VRF Aware System Message Logging

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 8 Feature Information for VRF Aware System Message Logging

Feature Name	Releases	Feature Information
VRF Aware System Message Logging (Syslog)	Cisco IOS XE Release 2.2	The VRF Aware System Message Logging (Syslog) feature allows a router to send syslog messages to a syslog server host connected through a VPN VRF interface. In Cisco IOS XE Release 2.2, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following command was modified: **logging host**.

Glossary

CE router --customer edge router. A router on the border between a VPN provider and a VPN customer that belongs to the customer.

LSR --label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

MPLS --Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS VPN --Multiprotocol Label Switching Virtual Private Network. An IP network infrastructure delivering private network services over a public infrastructure using a Layer 3 backbone. Using MPLS VPNs in a Cisco network provides the capability to deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers.

PE router --provider edge router. A router on the border between a VPN provider and a VPN customer that belongs to the provider.

VPN --Virtual Private Network. A group of sites that, as the result of a set of administrative policies, are able to communicate with each other over a shared backbone network. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone. *Seealso* MPLS VPN.

VRF --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

MPLS VPN--L3VPN over GRE

The MPLS VPN--L3VPN over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network.

The MPLS VPN--L3VPN over GRE feature utilizes MPLS over generic routing encapsulation (MPLSoGRE) to encapsulate MPLS packets inside IP tunnels. This action creates a virtual point-to-point link across non-MPLS networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MPLS VPN--L3VPN over GRE

Before you configure the MPLS VPN--L3VPN over GRE feature, ensure that your MPLS Virtual Private Network (VPN) is configured and working properly. See the Configuring MPLS Layer 3 VPNs module for information about setting up MPLS VPNs.

Ensure that the following routing protocols are configured and working properly:

- Label Distribution Protocol (LDP)--for MPLS label distribution. See MPLS Label Distribution Protocol Overview
- Multiprotocol Border Gateway Protocol (MP-BGP)--for VPN route and label distribution. See Configuring MPLS Layer 3 VPNs

Restrictions for MPLS VPN--L3VPN over GRE

The MPLS VPN--L3VPN over GRE feature does not support the following:

- Quality of service (QoS) service policies configured on the tunnel interface; they are supported on the physical or subinterface
- GRE options: sequencing, checksum, and source route
- IPv6 GRE
- Advanced features such as Carrier Supporting Carrier (CSC) and Interautonomous System (Inter-AS)
- For PE-to-PE tunneling, configure tunnels with the same source address if you are running a release earlier than Cisco IOS Release 15.2(1)S.
- For PE-to-PE tunneling, configure tunnels with the same destination address

Information About MPLS VPN--L3VPN over GRE

The MPLS VPN--L3VPN over GRE feature provides a mechanism for tunneling MPLS packets over non-MPLS networks.

MPLS VPN--L3VPN over GRE allows you to create a GRE tunnel across a non-MPLS network. The MPLS packets are encapsulated within the GRE tunnel packets, and the encapsulated packets traverse the non-MPLS network through the GRE tunnel. When GRE tunnel packets are received at the other side of the non-MPLS network, the GRE tunnel packet header is removed and the inner MPLS packet is forwarded to its final destination.

The MPLS VPN--L3VPN over GRE feature supports three GRE tunnel configurations:

- PE-to-PE Tunneling, page 128
- P-to-PE Tunneling, page 129
- P-to-P Tunneling, page 129

PE-to-PE Tunneling

The provider edge-to-provider edge (PE-to-PE) tunneling configuration provides a scalable way to connect multiple customer networks across a non-MPLS network. With this configuration, traffic that is destined to multiple customer networks is multiplexed through a single GRE tunnel.

Note A similar nonscalable alternative is to connect each customer network through separate GRE tunnels (for example, connecting one customer network for each GRE tunnel).

As shown in the figure below, the PE routers assign VPN routing and forwarding (VRF) numbers to the customer edge (CE) routers on each side of the non-MPLS network.

The PE routers use routing protocols such as BGP, OSPF, or Routing Information Protocol (RIP) to learn about the IP networks behind the CE routers. The routes to the IP networks behind the CE routers are stored in the associated CE router's VRF routing table.

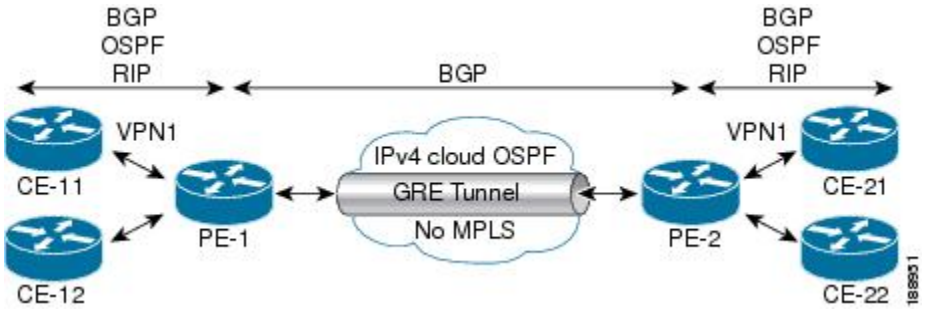
The PE router on one side of the non-MPLS network uses the routing protocols (that are operating within the non-MPLS network) to learn about the PE router on the other side of the non-MPLS network. The

learned routes that are established between the PE routers are then stored in the main or default routing table.

The opposing PE router uses BGP to learn about the routes that are associated with the customer networks behind the PE routers. These learned routes are not known to the non-MPLS network.

For this example, BGP defines a static route to the BGP neighbor (the opposing PE router) through the GRE tunnel that spans the non-MPLS network. Because the routes that are learned by the BGP neighbor include the GRE tunnel next hop, all customer network traffic is sent using the GRE tunnel.

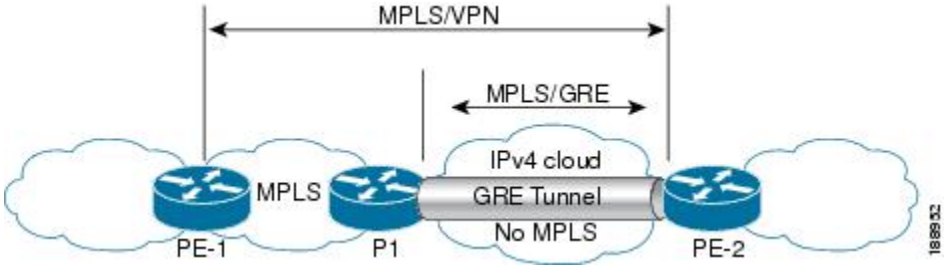
Figure 7 PE-to-PE Tunneling



P-to-PE Tunneling

As shown in the figure below, the provider-to-provider edge (P-to-PE) tunneling configuration provides a way to connect a PE router (P1) to an MPLS segment (PE-2) across a non-MPLS network. In this configuration, MPLS traffic that is destined to the other side of the non-MPLS network is sent through a single GRE tunnel.

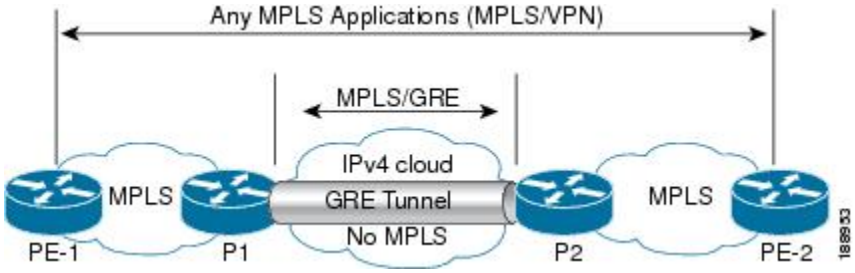
Figure 8 P-to-PE Tunneling



P-to-P Tunneling

As shown in the figure below, the provider-to-provider (P-to-P) configuration provides a method of connecting two MPLS segments (P1 to P2) across a non-MPLS network. In this configuration, MPLS traffic that is destined to the other side of the non-MPLS network is sent through a single GRE tunnel.

Figure 9 P-to-P Tunneling



How to Configure MPLS VPN--L3VPN over GRE

Configuring the MPLS VPN--L3VPN over GRE Tunnel Interface

To configure the MPLS VPN--L3VPN over GRE feature, you must create a GRE tunnel to span the non-MPLS networks. You must perform this procedure on the devices located at both ends of the GRE tunnel.

Before configuring the MPLS VPN--L3VPN over GRE feature, ensure that your MPLS VPN and the appropriate routing protocols are configured and working properly. See the Prerequisites for MPLS VPN--L3VPN over GRE, page 127.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ip address** *ip-address*
5. **tunnel source** *source-address*
6. **tunnel destination** *destination-address*
7. **mpls ip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *tunnel-number* **Example:** `Router(config)# interface tunnel 1`	Creates a tunnel on the specified interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	Assigns an IP address to the tunnel interface.
Step 5	**tunnel source** *source-address* **Example:** `Router(config-if)# tunnel source 10.1.1.1`	Specifies the tunnel's source IP address.
Step 6	**tunnel destination** *destination-address* **Example:** `Router(config-if)# tunnel destination 10.1.1.2`	Specifies the tunnel's destination IP address.
Step 7	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS on the tunnel's physical interface.

- Examples, page 131

Examples

The following example shows a GRE tunnel configuration that spans a non-MPLS network. This example shows the tunnel configuration on the PE devices (PE1 and PE2) located at both ends of the tunnel:

PE1 Configuration

```
Router# configure terminal
Router(config)# interface Tunnel 1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# tunnel source 10.0.0.1
Router(config-if)# tunnel destination 10.0.0.2
Router(config-if)# mpls ip
```

PE2 Configuration

```
Router# configure terminal
Router(config)# interface Tunnel 1
Router(config-if)# ip address 10.1.1.2 255.255.255.0
Router(config-if)# tunnel source 10.0.0.2
Router(config-if)# tunnel destination 10.0.0.1
Router(config-if)# mpls ip
```

Configuration Examples for MPLS VPN--L3VPN over GRE

MPLS Configuration with MPLS VPN--L3VPN over GRE Example

The following basic MPLS configuration example uses a GRE tunnel to span a non-MPLS network. This example is similar to the configuration shown in the first figure above.

PE1 Configuration

```
!
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
interface loopback 0
ip address 10.2.2.2 255.255.255.255
!
interface GigabitEthernet 0/1/2
ip address 10.1.1.1 255.255.255.0
!
interface Tunnel 1
ip address 10.0.0.1 255.255.255.0
tunnel source 10.1.1.1
tunnel destination 10.1.1.2
mpls ip
!
interface GigabitEthernet 0/1/3
ip vrf forwarding vpn1
ip address 10.10.0.1 255.255.255.0
!
router bgp 100
neighbor 10.5.5.5 remote-as 100
neighbor 10.5.5.5 update-source loopback0
!
address-family vpnv4
neighbor 10.5.5.5 activate
neighbor 10.5.5.5 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 10.10.0.2 remote-as 20
neighbor 10.10.0.2 activate
!
```

PE2 Configuration

```
!
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
interface loopback 0
ip address 10.5.5.5 255.255.255.255
!
interface GigabitEthernet 0/1/1
ip address 10.1.1.2 255.255.255.0
!
```

```
interface Tunnel 1
ip address 10.0.0.2 255.255.255.0
tunnel source 10.1.1.2
tunnel destination 10.1.1.1
mpls ip
!
interface GigabitEthernet 0/0/5
ip vrf forwarding vpn1
ip address 10.1.2.1 255.255.255.0
!
router bgp 100
neighbor 10.2.2.2 remote-as 100
neighbor 10.2.2.2 update-source loopback0
!
address-family vpnv4
neighbor 10.2.2.2 activate
neighbor 10.2.2.2 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 10.1.2.2 remote-as 30
neighbor 10.1.2.2 activate
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Multiprotocol Label Switching (MPLS) commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
Setting up MPLS VPN networks	Configuring MPLS Layer 3 VPNs
Label Distribution Protocol	MPLS Label Distribution Protocol Overview
Multiprotocol Border Gateway Protocol (MP-BGP)	Configuring MPLS Layer 3 VPNs
Configuring L3 VPN over mGRE Tunnels	Dynamic Layer-3 VPNs with Multipoint GRE Tunnels

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for MPLS VPN--L3VPN over GRE

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 9 Feature Information for MPLS VPN--L3VPN over GRE

Feature Name	Releases	Feature Information
MPLS VPN--L3VPN over GRE feature	12.0(22)S 12.2(13)T 12.0(26)S 12.2(33)SRE Cisco IOS XE Release 2.1 15.2(1)S	The MPLS VPN--L3VPN over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network. In Cisco IOS Release 15.2(1)S, you can configure tunnels with the same source address in a PE-to-PE tunneling configuration. This feature uses no new or modified commands.

MPLS VPN Half-Duplex VRF

The MPLS VPN Half-Duplex VRF feature provides scalable hub-and-spoke connectivity for subscribers of an Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) service. This feature addresses the limitations of hub-and-spoke topologies by removing the requirement of one virtual routing and forwarding (VRF) instance per spoke. This feature also ensures that subscriber traffic always traverses the central link between the wholesale service provider and the Internet service provider (ISP), whether the subscriber traffic is being routed to a remote network by way of the upstream ISP or to another locally or remotely connected subscriber.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring MPLS VPN Half-Duplex VRF

You must have a working MPLS core network.

Restrictions for MPLS VPN Half-Duplex VRF

The following features are not supported on interfaces configured with the MPLS VPN Half-Duplex VRF feature:

- Multicast

- MPLS VPN Carrier Supporting Carrier
- MPLS VPN Interautonomous Systems

Information About Configuring MPLS VPN Half-Duplex VRF

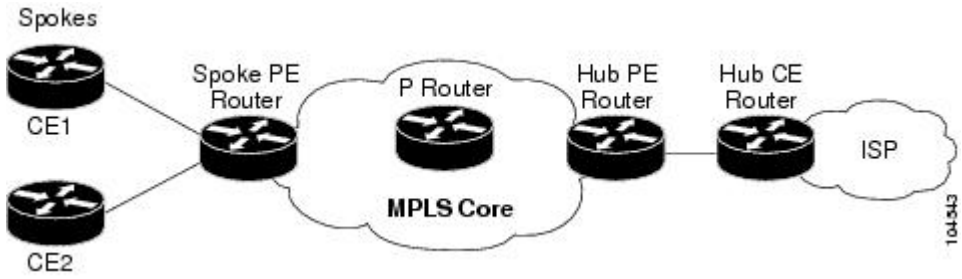
MPLS VPN Half-Duplex VRF Overview

The MPLS VPN Half-Duplex VRF feature provides:

- The MPLS VPN Half-Duplex VRF feature prevents local connectivity between subscribers at the spoke provider edge (PE) router and ensures that a hub site provides subscriber connectivity. Any sites that connect to the same PE router must forward intersite traffic using the hub site. This ensures that the routing done at the spoke site moves from the access-side interface to the network-side interface or from the network-side interface to the access-side interface, but never from the access-side interface to the access-side interface.
- The MPLS VPN Half-Duplex VRF feature prevents situations where the PE router locally switches the spokes without passing the traffic through the upstream ISP. This prevents subscribers from directly connecting to each other, which causes the wholesale service provider to lose revenue.
- The MPLS VPN Half-Duplex VRF feature improves scalability by removing the requirement of one VRF per spoke. If the feature is not configured, when spokes are connected to the same PE router each spoke is configured in a separate VRF to ensure that the traffic between the spokes traverses the central link between the wholesale service provider and the ISP. However, this configuration is not scalable. When many spokes are connected to the same PE router, configuration of VRFs for each spoke becomes quite complex and greatly increases memory usage. This is especially true in large-scale wholesale service provider environments that support high-density remote access to Layer 3 VPNs.

The figure below shows a sample hub-and-spoke topology.

Figure 10 Hub-and-Spoke Topology



Upstream and Downstream VRFs

The MPLS VPN Half-Duplex VRF feature uses two unidirectional VRFs to forward IP traffic between the spokes and the hub PE router:

- The upstream VRF forwards IP traffic from the spokes toward the hub PE router. This VRF typically contains only a default route but might also contain summary routes and several default routes. The default route points to the interface on the hub PE router that connects to the upstream ISP. The router dynamically learns about the default route from the routing updates that the hub PE router or home gateway sends.

Note Although the upstream VRF is typically populated from the hub, it is possible also to have a separate local upstream interface on the spoke PE for a different local service that would not be required to go through the hub: for example, a local Domain Name System (DNS) or game server service.

- The downstream VRF forwards traffic from the hub PE router back to the spokes. This VRF can contain:
  - PPP peer routes for the spokes and per-user static routes received from the authentication, authorization, and accounting (AAA) server or from the Dynamic Host Control Protocol (DHCP) server
  - Routes imported from the hub PE router
  - Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), or Enhanced Interior Gateway Routing Protocol (EIGRP) dynamic routes for the spokes

The spoke PE router redistributes routes from the downstream VRF into Multiprotocol Border Gateway Protocol (MP-BGP). That router typically advertises a summary route across the MPLS core for the connected spokes. The VRF configured on the hub PE router imports the advertised summary route.

Reverse Path Forwarding Check

The Reverse Path Forwarding (RPF) check ensures that an IP packet that enters a router uses the correct inbound interface. The MPLS VPN Half-Duplex VRF feature supports unicast RPF check on the spoke-side interfaces. Because different VRFs are used for downstream and upstream forwarding, the RPF mechanism ensures that source address checks occur in the downstream VRF.

Unicast RPF is not on by default. You need to enable it, as described in Configuring Unicast Reverse Path Forwarding .

How to Configure MPLS VPN Half-Duplex VRF

Configuring the Upstream and Downstream VRFs on the Spoke PE Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit-address-family**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition vrf1`	Configures a VRF routing table and enters VRF configuration mode. • The *vrf-name* argument is the name of the VRF.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF. • The *route-distinguisher* argument specifies to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher in either of these formats: ◦ 16-bit autonomous system number (ASN): your 32-bit number For example, 101:3. ◦ 32-bit IP address: your 16-bit number For example, 192.168.122.15:1.

	Command or Action	Purpose
Step 5	**address-family** {**ipv4** | **ipv6**} **Example:** `Router(config-vrf) address-family ipv4`	Enters VRF address family configuration mode to specify an address family for a VRF. • The **ipv4** keyword specifies an IPv4 address family for a VRF. • The **ipv6** keyword specifies an IPv6 address family for a VRF. **Note** The MPLS VPN Half Duplex VRF feature supports only the IPv4 address family.
Step 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf-af)# route-target both 100:2`	Creates a route-target extended community for a VRF. • The **import** keyword specifies to import routing information from the target VPN extended community. • The **export** keyword specifies to export routing information to the target VPN extended community. • The **both** keyword specifies to import both import and export routing information to the target VPN extended community. • The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.
Step 7	**exit-address-family** **Example:** `Router(config-vrf-af)# exit-address-family`	Exits VRF address family configuration mode.
Step 8	**end** **Example:** `Router(config-vrf)# end`	Exits to privileged EXEC mode.

Associating a VRF with an Interface

Perform the following task to associate a VRF with an interface, which activates the VRF.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name* [**downstream** *vrf-name2*
5. **ip address** *ip-address mask* [**secondary**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/1`	Configures an interface type and enters interface configuration mode. • The *type* argument identifies the type of interface to be configured. • The *number* argument identifies the port, connector, or interface card number.
Step 4	**vrf forwarding** *vrf-name* [**downstream** *vrf-name2* **Example:** `Router(config-if)# vrf forwarding vrf1`	Associates a VRF with an interface or subinterface. • The *vrf-name* argument is the name of the VRF. • The **downstream** *vrf-name2* keyword and argument combination is the name of the downstream VRF into which peer and per-user routes are installed.
Step 5	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.24.24.24 255.255.255.255`	Sets a primary or secondary IP address for an interface. • The *ip-address* argument is the IP address. • The *mask* argument is the mask of the associated IP subnet. • The **secondary** keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
Step 6	**end** **Example:** `Router(config-if) end`	Exits to privileged EXEC mode.

Configuring the Downstream VRF for an AAA Server

To configure the downstream VRF for an AAA (RADIUS) server in broadband or remote access situations, enter the following Cisco attribute value:

lcp:interface-config=ip vrf forwarding U downstream D

In standard VPN situations, enter instead the following Cisco attribute value:

ip:vrf-id=U downstream D

Verifying MPLS VPN Half-Duplex VRF Configuration

SUMMARY STEPS

1. **show vrf** [**ipv4** | **ipv6**] [**brief** | **detail** | **id** | **interfaces** | **lock** | **select**] [*vrf-name*]
2. **show ip route vrf** *vrf-name*
3. **show running-config** [**interface** *type number*]

DETAILED STEPS

Step 1 **show vrf** [**ipv4** | **ipv6**] [**brief** | **detail** | **id** | **interfaces** | **lock** | **select**] [*vrf-name*]

Use this command to display information about all of the VRFs configured on the router, including the downstream VRF for each associated interface or virtual access interface (VAI):

Example:

```
Router# show vrf
Name     Default RD     Interfaces
Down     100:1          POS3/0/3 [D]
                        POS3/0/1 [D]
         100:3          Loopback2
                        Virtual-Access3 [D]
                        Virtual-Access4 [D]
Up       100:2          POS3/0/3
                        POS3/0/1
         100:4          Virtual-Access3
```

Use the **show vrf detail** *vrf-name* command to display detailed information about the VRF you specify, including all interfaces, subinterfaces, and VAIs associated with the VRF.

If you do not specify a value for the *vrf-name* argument, detailed information about all of the VRFs configured on the router appears.

The following example shows how to display detailed information for the VRF called vrf1, in a broadband or remote access case:

Example:

```
Router# show vrf detail vrf1
VRF D; default RD 2:0; default VPNID <not set>
  Interfaces:
         Loopback2           Virtual-Access3 [D]  Virtual-Access4 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:0
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
VRF U; default RD 2:1; default VPNID <not set>
  Interfaces:
```

```
    Virtual-Access3          Virtual-Access4
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
```

The following example shows the VRF detail in a standard VPN situation:

Example:

```
Router# show vrf detail
VRF Down; default RD 100:1; default VPNID <not set> VRF Table ID = 1
  Description: import only from hub-pe
  Interfaces:
    Pos3/0/3 [D]        Pos3/0/1:0.1 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:0
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
    VRF Up; default RD 100:2; default VPNID <not set> VRF Table ID = 2
  Interfaces:
    Pos3/0/1            Pos3/0/3
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

Step 2 **show ip route vrf** *vrf-name*

Use this command to display the IP routing table for the VRF you specify, and information about the per-user routes installed in the downstream VRF.

The following example shows how to display the routing table for the downstream VRF named D, in a broadband or remote access situation:

Example:

```
Router# show ip route vrf D

Routing Table: D
Codes: C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
U         10.0.0.2/32 [1/0] via 10.0.0.1
S         10.0.0.0/8 is directly connected, Null0
U         10.0.0.5/32 [1/0] via 10.0.0.2
C         10.8.1.2/32 is directly connected, Virtual-Access4
C         10.8.1.1/32 is directly connected, Virtual-Access3
```

The following example shows how to display the routing table for the downstream VRF named Down, in a standard VPN situation:

Example:

```
Router# show ip route vrf Down

Routing Table: Down
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.13.13.13 to network 0.0.0.0
C     10.2.0.0/8 is directly connected, Pos3/0/3
     10.3.0.0/32 is subnetted, 1 subnets
B       10.4.16.16 [200/0] via 10.13.13.13, 1w3d
B     10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
C     10.0.0.0/8 is directly connected, Pos3/0/1
    10.7.0.0/16 is subnetted, 1 subnets
B         10.7.0.0 [20/0] via 10.0.0.2, 1w3d
     10.0.6.0/32 is subnetted, 1 subnets
B       10.0.6.14 [20/0] via 10.0.0.2, 1w3d
     10.8.0.0/32 is subnetted, 1 subnets
B       10.8.15.15 [20/0] via 10.0.0.2, 1w3d
B*   0.0.0.0/0 [200/0] via 10.0.0.13, 1w3d
```

The following example shows how to display the routing table for the upstream VRF named U in a broadband or remote access situation:

Example:

```
Router# show ip route vrf U
Routing Table: U
Codes: C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 192.168.0.20 to network 0.0.0.0
    10.0.0.0/32 is subnetted, 1 subnets
C         10.0.0.8 is directly connected, Loopback2
B*   0.0.0.0/0 [200/0] via 192.168.0.20, 1w5d
```

The following example shows how to display the routing table for the upstream VRF named Up in a standard VPN situation:

Example:

```
Router# show ip route vrf Up
Routing Table: Up
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.13.13.13 to network 0.0.0.0
    10.2.0.0/32 is subnetted, 1 subnets
C         10.2.0.1 is directly connected, Pos3/0/3
     10.3.0.0/32 is subnetted, 1 subnets
B       10.3.16.16 [200/0] via 10.13.13.13, 1w3d
B     10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
    10.0.0.0/32 is subnetted, 1 subnets
```

```
C        10.0.0.1 is directly connected, Pos3/0/1
B*   0.0.0.0/0 [200/0] via 10.13.13.13, 1w3d
```

Step 3 **show running-config** [**interface** *type number*]

Use this command to display information about the interface you specify, including information about the associated upstream and downstream VRFs.

The following example shows how to display information about subinterface POS 3/0/1:

Example:

```
Router# show running-config interface POS 3/0/1
Building configuration...
Current configuration : 4261 bytes
!
interface POS3/0/1
ip vrf forwarding Up downstream Down
ip address 10.0.0.1 255.0.0.0
end
```

Configuration Examples for MPLS VPN Half-Duplex VRF

Example Configuring the Upstream and Downstream VRFs on the Spoke PE Router

The following example configures an upstream VRF named Up:

```
Router> enable
Router# configure terminal
Router(config)# vrf definition Up
Router(config-vrf)# rd 1:0
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# route-target import 1:0
Router(config-vrf-af)# exit-address-family
```

The following example configures a downstream VRF named Down:

```
Router> enable
Router# configure terminal
Router(config)# vrf definition Down
Router(config-vrf)# rd 1:8
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# route-target import 1:8
Router(config-vrf-af)# exit-address-family
```

Example Associating a VRF with an Interface

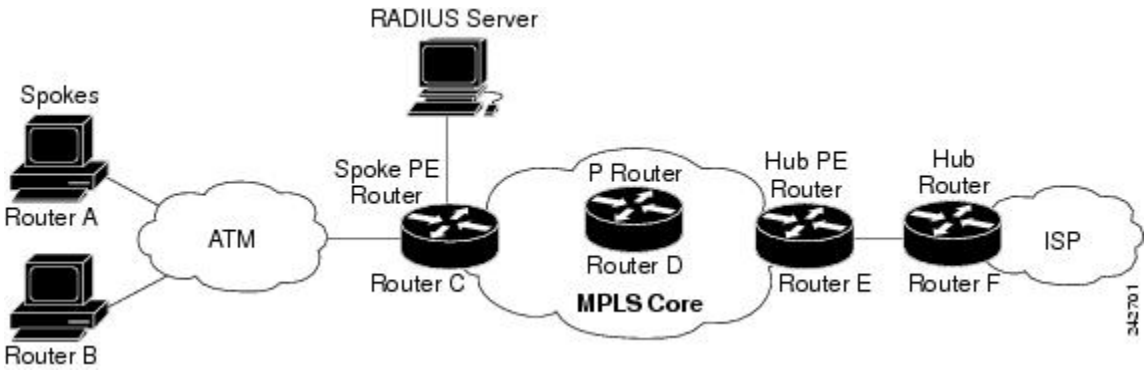
The following example associates the VRF named Up with POS 3/0/1 subinterface and specifies the downstream VRF named Down:

```
Router> enable
Router# configure terminal
Router(config)# interface POS 3/0/1
Router(config-if)# vrf forwarding Up downstream Down
Router(config-if)# ip address 10.0.0.1 255.0.0.0
```

Example Configuring MPLS VPN Half-Duplex VRF Using Static CE-PE Routing

This example uses the hub-and-spoke topology shown in the figure below with local authentication (that is, the RADIUS server is not used):

Figure 11 Sample Topology




```
vrf definition D
 rd 1:8
 address-family ipv4
 route-target export 1:100
 exit-address-family
!
vrf definition U
 rd 1:0
 address-family ipv4
 route-target import 1:0
 exit-address-family
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback 2
 vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM 2/0
 description Mze ATM3/1/2
 no ip address
```

```
 no atm ilmi-keepalive
 pvc 0/16 ilmi
!
 pvc 3/100
  protocol pppoe
!
pvc 3/101
  protocol pppoe
!
```

Example Configuring MPLS VPN Half-Duplex VRF Using RADIUS Server and Static CE-PE Routing

The following example shows how to connect two Point-to-Point Protocol over Ethernet (PPPoE) clients to a single VRF pair on the spoke PE router named Router C. Although both PPPoE clients are configured in the same VRF, all communication occurs using the hub PE router. Half-duplex VRFs are configured on the spoke PE. The client configuration is downloaded to the spoke PE from the RADIUS server.

This example uses the hub-and-spoke topology shown in the figure above.

Note The wholesale provider can forward the user authentication request to the corresponding ISP. If the ISP authenticates the user, the wholesale provider appends the VRF information to the request that goes back to the PE router.

```
aaa new-model
!
aaa group server radius R
 server 10.0.20.26 auth-port 1812 acct-port 1813
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
vrf defintion D
 description Downstream VRF - to spokes
 rd 1:8
 address-family ipv4
 route-target export 1:100
 exit-address-family
!
vrf definition U
 description Upstream VRF - to hub
 rd 1:0
 address-family ipv4
 route-target import 1:0
 exit-address-family
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback2
 vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM2/0
  pvc 3/100
  protocol pppoe
 !
pvc 3/101
  protocol pppoe
```

```
 !
interface virtual-template 1
 no ip address
 ppp authentication chap
!
router bgp 1
 no synchronization
 neighbor 172.16.0.34 remote-as 1
 neighbor 172.16.0.34 update-source Loopback0
 no auto-summary
 !
address-family vpnv4
  neighbor 172.16.0.34 activate
  neighbor 172.16.0.34 send-community extended
  auto-summary
  exit-address-family
 !
address-family ipv4 vrf U
  no auto-summary
  no synchronization
  exit-address-family
!
address-family ipv4 vrf D
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool U-pool 10.8.1.1 2.8.1.100
ip route vrf D 10.0.0.0 255.0.0.0 Null0
!
radius-server host 10.0.20.26 auth-port 1812 acct-port 1813
radius-server key cisco
```

Example Configuring MPLS VPN Half-Duplex VRF Using Dynamic CE-PE Routing

The following example shows how to use OSPF to dynamically advertise the routes on the spoke sites.

This example uses the hub-and-spoke topology shown in the figure above.

Creating the VRFs

```
vrf definition Down
rd 100:1
address-family ipv4
route-target export 100:0
exit-address-family
!
vrf definition Up
rd 100:2
address-family ipv4
route-target import 100:1
exit-address-family
```

Enabling MPLS

```
mpls ldp graceful-restart
mpls ldp router-id Loopback0 force
mpls label protocol ldp
```

Configuring BGP Toward Core

```
router bgp 100
 no bgp default ipv4-unicast
```

```
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.13.13.13 remote-as 100
 neighbor 10.13.13.13 update-source Loopback0
 !
 address-family vpnv4
 neighbor 10.13.13.13 activate
 neighbor 10.13.13.13 send-community extended
 bgp scan-time import 5
 exit-address-family
```

Configuring BGP Toward Edge

```
address-family ipv4 vrf Up
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf Down
redistribute ospf 1000 vrf Down
no auto-summary
no synchronization
exit-address-family
```

Spoke PE's Core-Facing Interfaces and Processes

```
interface Loopback 0
 ip address 10.11.11.11 255.255.255.255
!
interface POS 3/0/2
 ip address 10.0.1.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 10.11.11.11 0.0.0.0 area 100
 network 10.0.1.0 0.255.255.255 area 100
```

Spoke PE's Edge-Facing Interfaces and Processes

```
interface Loopback 100
vrf forwarding Down
 ip address 10.22.22.22 255.255.255.255
!
interface POS 3/0/1
vrf forwarding Up downstream Down
 ip address 10.0.0.1 255.0.0.0
!
interface POS 3/0/3
vrf forwarding Up downstream Down
 ip address 10.2.0.1 255.0.0.0
!
router ospf 1000 vrf Down
 router-id 10.22.22.22
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 redistribute bgp 100 metric-type 1 subnets
 network 10.22.22.22 0.0.0.0 area 300
 network 10.0.0.0 0.255.255.255 area 300
 network 10.2.0.0 0.255.255.255 area 300
 default-information originate
```

Additional References

Related Documents

Related Topic	Document Title
MPLS VPNs	Configuring MPLS Layer 3 VPNs
MPLS commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
Configuring IPv4 and IPv6 VRFs	MPLS VPN--VRF CLI for IPv4 and IPv6 VPNs
Unicast Reverse Path Forwarding	Configuring Unicast Reverse Path Forwarding

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2547	BGP/MPLS VPNs

Technical Assistance

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

Feature Information for MPLS VPN Half-Duplex VRF

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 10 Feature Information for MPLS VPN Half-Duplex VRF

Feature Name	Releases	Feature Information
MPLS VPN - Half Duplex VRF (HDVRF) Support with Static Routing	Cisco IOS XE Release 2.5	This feature ensures that VPN clients that connect to the same PE router at the edge of the MPLS VPN use the hub site to communicate. In Cisco IOS XE Release 2.5, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Feature Name	Releases	Feature Information
MPLS VPN Half-Duplex VRF	Cisco IOS XE Release 2.5	In Cisco IOS XE Release 2.5, this feature, with support for dynamic routing protocols, was integrated into the XE train. The following commands were introduced or modified: **ip vrf forwarding** (interface configuration), **show ip interface**, **show vrf**.