



# Configuring MPLS Layer 3 VPNs

---

**First Published: May 2, 2005**

**Last Updated: August 26, 2008**

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 for MPLS Layer 3 VPNs”](#) section on page 36.

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

## Contents

- [Prerequisites for MPLS Layer 3 VPNs, page 2](#)
- [Restrictions for MPLS Layer 3 VPNs, page 2](#)
- [Information about MPLS Layer 3 VPNs](#)
- [How to Configure MPLS Layer 3 VPNs](#)
- [Configuration Examples for MPLS VPNs, page 29](#)
- [Additional References, page 35](#)
- [Feature Information for MPLS Layer 3 VPNs, page 36](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS Layer 3 VPNs

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

## 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 releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.xT, 12.xM, and 12.0S. 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 releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later. 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  
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

Before configuring MPLS Layer 3 VPNs, you should understand the following concepts:

- [MPLS VPN Definition, page 4](#)
- [How an MPLS VPN Works, page 5](#)
- [Major Components of MPLS VPNs, page 7](#)
- [Benefits of an MPLS VPN, page 7](#)

## 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.

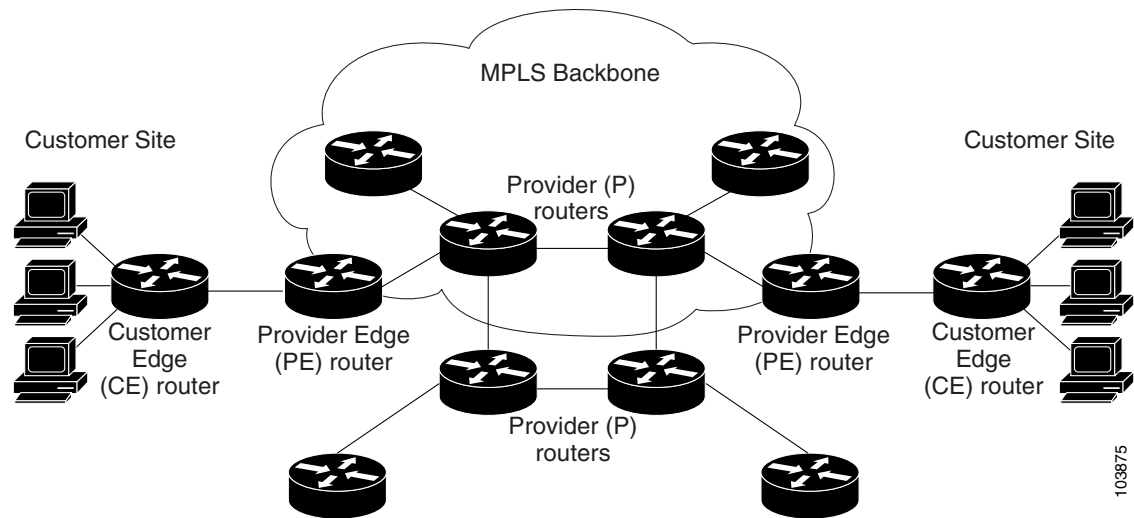
MPLS VPNs are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS VPN, only the service provider's edge router that provides services to the customer site needs to be updated.

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.

[Figure 1](#) shows a basic MPLS VPN.

**Figure 1 Basic MPLS VPN Terminology**



103875

## 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/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 CEF 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 CEF table for each VRF. A separate set of routing and CEF 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. In an EIGRP PE-CE environment, when an EIGRP internal route is redistributed into BGP by one PE, then back into EIGRP by another PE, the originating router-id for the route is set to the router-id of the second PE, replacing the original internal router-id.

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (refer to 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 CEF 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, including:

**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

To configure and verify VPNs, perform the tasks described in the following sections:

- [Configuring the Core Network, page 9](#) (required)
- [Connecting the MPLS VPN Customers, page 13](#) (required)
- [Verifying Connectivity Between MPLS VPN Sites, page 27](#) (optional)

### Configuring the Core Network

Configuring the core network includes the following tasks:

- [Assessing the Needs of MPLS VPN Customers, page 9](#) (required)
- [Configuring Routing Protocols in the Core, page 10](#) (required)
- [Configuring MPLS in the Core, page 10](#) (required)
- [Determining if CEF Is Enabled in the Core, page 10](#) (required)
- [Configuring Multiprotocol BGP on the PE Routers and Route Reflectors, page 11](#) (required)

### 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.
3. Determine if you need MPLS High Availability support.
4. Determine if you need BGP load sharing and redundant paths.

## 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: <ul style="list-style-type: none"> <li>• How many customers do you need to support?</li> <li>• How many VPNs are needed per customer?</li> <li>• How many virtual routing and forwarding instances are there for each VPN?</li> </ul>
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 IOS releases. Contact Cisco Support for the exact requirements and hardware support.
Step 4	Determine if you need BGP load sharing and redundant paths in the MPLS VPN core.	See <a href="#">Load Sharing MPLS VPN Traffic</a> 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](#).

## Determining if CEF Is Enabled in the Core

Cisco Express Forwarding (CEF) must be enabled all routers in the core, including the PE routers. For information about how to determine if CEF is enabled, see [Configuring Basic Cisco Express Forwarding](#).

## 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 vpv4** [**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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router bgp 100	Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> 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.</li> </ul>
Step 4	<b>no bgp default ipv4-unicast</b>  <b>Example:</b> Router(config-router)# no bgp default ipv4-unicast	(Optional) Disables the IPv4 unicast address family on all neighbors. <ul style="list-style-type: none"> <li>• Use the <b>no</b> form of the <b>bgp default ipv4-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>

	Command or Action	Purpose
Step 5	<pre>neighbor {ip-address   peer-group-name} remote-as as-number</pre> <p><b>Example:</b> Router(config-router)# neighbor pp.0.0.1 remote-as 100</p>	<p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>
Step 6	<pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b> Router(config-router)# neighbor pp.0.0.1 activate</p>	<p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>
Step 7	<pre>address-family vpnv4 [unicast]</pre> <p><b>Example:</b> Router(config-router)# address-family vpnv4</p>	<p>Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>
Step 8	<pre>neighbor {ip-address   peer-group-name} send-community extended</pre> <p><b>Example:</b> Router(config-router-af)# neighbor pp.0.0.1 send-community extended</p>	<p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>
Step 9	<pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b> Router(config-router-af)# neighbor pp.0.0.1 activate</p>	<p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>
Step 10	<pre>end</pre> <p><b>Example:</b> Router(config-router-af)# end</p>	<p>(Optional) Exits to privileged EXEC mode.</p>

## 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

To connect the MPLS VPN customers to the VPN, perform the following tasks:

- [Defining VRFs on the PE Routers to Enable Customer Connectivity, page 13](#) (required)
- [Configuring VRF Interfaces on PE Routers for Each VPN Customer, page 14](#) (required)
- [Configuring Routing Protocols Between the PE and CE Routers, page 15](#) (required)

### 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip vrf</b> <i>vrf-name</i>  <b>Example:</b> Router(config)# ip vrf vpn1	Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode. <ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>

	Command or Action	Purpose
Step 4	<pre>rd route-distinguisher</pre> <p><b>Example:</b> Router(config-vrf)# rd 100:1</p>	<p>Creates routing and forwarding tables.</p> <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> 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: <ul style="list-style-type: none"> <li>16-bit AS number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>
Step 5	<pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b> Router(config-vrf)# route-target import 100:1</p>	<p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> 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.</li> </ul>
Step 6	<pre>import map route-map</pre> <p><b>Example:</b> Router(config-vrf)# import map vpn1-route-map</p>	<p>(Optional) Configures an import route map for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config-vrf)# exit</p>	<p>(Optional) Exits to global configuration mode.</p>

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface Ethernet 5/0	Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul>
Step 4	<b>ip vrf forwarding</b> <i>vrf-name</i>  <b>Example:</b> Router(config-if)# ip vrf forwarding vpn1	Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>
Step 5	<b>end</b>  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 25](#)

## 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

- enable**
- configure terminal**
- 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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>router bgp</b> <i>as-number</i></p> <p><b>Example:</b> Router(config)# router bgp 100</p>	<p>Configures a BGP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>• The <i>as-number</i> 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.</li> </ul>
Step 4	<p><b>address-family ipv4</b> [<b>multicast</b>   <b>unicast</b>   <b>vrf vrf-name</b>]</p> <p><b>Example:</b> Router(config-router)# address-family ipv4 vrf vpn1</p>	<p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>• The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>• The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>• The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>



	Command or Action	Purpose
Step 5	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b> Router(config-router-af)# neighbor pp.0.0.1 remote-as 200</p>	<p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>
Step 6	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>activate</b></p> <p><b>Example:</b> Router(config-router-af)# neighbor pp.0.0.1 activate</p>	<p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>
Step 7	<p><b>exit-address-family</b></p> <p><b>Example:</b> Router(config-router-af)# exit-address-family</p>	<p>Exits address family configuration mode.</p>
Step 8	<p><b>end</b></p> <p><b>Example:</b> Router(config-router)# end</p>	<p>(Optional) Exits to privileged EXEC mode.</p>

### 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

- enable**
- configure terminal**
- router rip**
- version** {1 | 2}
- address-family** ipv4 [multicast | unicast | vrf *vrf-name*]
- network** *ip-address*
- 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**]
- exit-address-family**
- end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>router rip</code>  <b>Example:</b> Router(config)# router rip	Enables RIP.
Step 4	<code>version {1   2}</code>  <b>Example:</b> Router(config-router)# version 2	Specifies a Routing Information Protocol (RIP) version used globally by the router.
Step 5	<code>address-family ipv4 [multicast   unicast   vrf vrf-name]</code>  <b>Example:</b> Router(config-router)# address-family ipv4 vrf vpn1	Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 6	<code>network ip-address</code>  <b>Example:</b> Router(config-router-af)# network 192.168.7.0	Enables RIP on the PE-to-CE link.
Step 7	<code>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]</code>  <b>Example:</b> Router(config-router-af)# redistribute bgp 200	Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>For the RIPv2 routing protocol, use the <b>redistribute bgp as-number</b> command.</li> </ul> See the <a href="#">redistribute</a> command for information about other arguments and keywords.

	Command or Action	Purpose
Step 8	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode.
Step 9	<b>end</b>  <b>Example:</b> 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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>ip route vrf vrf-name</b></p> <p><b>Example:</b> Router(config)# ip route vrf 200</p>	<p>Defines static route parameters for every PE-to-CE session.</p>
Step 4	<p><b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b></p> <p><b>Example:</b> Router(config-router)# address-family ipv4 vrf vpn1</p>	<p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 5	<p><b>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]</b></p> <p><b>Example:</b> Router(config-router-af)# redistribute static</p>	<p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>To redistribute VRF static routes into the VRF BGP table, use the <b>redistribute static</b> command.</li> </ul> <p>See the command for information about other arguments and keywords.</p>
Step 6	<p><b>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]</b></p> <p><b>Example:</b> Router(config-router-af)# redistribute connected</p>	<p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>To redistribute directly connected networks into the VRF BGP table, use the <b>redistribute connected</b> command.</li> </ul> <p>See the <b>redistribute</b> command for information about other arguments and keywords.</p>

	Command or Action	Purpose
Step 7	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode.
Step 8	<b>end</b>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>router ospf process-id [vrf vpn-name]</pre> <p><b>Example:</b> Router(config)# router ospf 1 vrf grc</p>	<p>Enables OSPF routing and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>process-id</i> argument identifies the OSPF process.</li> <li>The <b>vrf</b> keyword and <i>vpn-name</i> argument identify a VPN. Create a separate OSPF process for each VRF that will receive VPN routes.</li> </ul>
Step 4	<pre>network ip-address wildcard-mask area area-id</pre> <p><b>Example:</b> Router(config-router)# network 192.168.129.16 0.0.0.3 area 20</p>	<p>Defines the interfaces on which OSPF runs and to defines the area ID for those interfaces.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument identifies the IP address.</li> <li>The <i>wildcard-mask</i> argument identifies the IP-address-type mask that includes “don't care” bits.</li> <li>The <i>area-id</i> 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 <i>area-id</i> argument.</li> </ul>
Step 5	<pre>address-family ipv4 [multicast   unicast   vrf vrf-name]</pre> <p><b>Example:</b> Router(config-router)# address-family ipv4 vrf vpn1</p>	<p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 6	<pre>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]</pre> <p><b>Example:</b> Router(config-router-af)# redistribute rip metric 1 subnets</p>	<p>Redistributes routes from one routing domain into another routing domain.</p> <p>You may need to include several protocols to ensure that all IBGP routes are distributed into the VRF.</p> <p>See the <b>redistribute</b> command for information about other arguments and keywords.</p>

	Command or Action	Purpose
Step 7	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode.
Step 8	<b>end</b>  <b>Example:</b> 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.

#### Prerequisites

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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp as-number</b>  <b>Example:</b> Router(config)# router bgp 10	Enters router configuration mode, and creates a BGP routing process.
Step 4	<b>no synchronization</b>  <b>Example:</b> Router(config-router)# no synchronization	Configures BGP to send advertisements without waiting to synchronize with the IGP.
Step 5	<b>neighbor ip-address remote-as as-number</b>  <b>Example:</b> Router(config-router)# neighbor 10.0.0.1 remote-as 10	Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>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.</li> </ul>
Step 6	<b>neighbor ip-address update-source loopback interface-number</b>  <b>Example:</b> Router(config-router)# neighbor 10.0.0.1 update-source loopback 0	Configures BGP to use any operational interface for TCP connections. <ul style="list-style-type: none"> <li>This configuration step is not required. However, the BGP routing process will be less susceptible to the affects of interface or link flapping.</li> </ul>
Step 7	<b>address-family vpnv4</b>  <b>Example:</b> 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	<b>neighbor ip-address activate</b>  <b>Example:</b> Router(config-router-af)# neighbor 10.0.0.1 activate	Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are activating the exchange of VPNv4 routing information between the PE routers.</li> </ul>
Step 9	<b>neighbor ip-address send-community extended</b>  <b>Example:</b> 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. <ul style="list-style-type: none"> <li>This step is required for the exchange of EIGRP extended community attributes.</li> </ul>



	Command or Action	Purpose
Step 10	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode and enters router configuration mode.
Step 11	<b>address-family ipv4 vrf vrf-name</b>  <b>Example:</b> Router(config-router)# address-family ipv4 vrf RED	Configures an IPv4 address-family for the EIGRP VRF and enters address family configuration mode. <ul style="list-style-type: none"> <li>An address-family VRF needs to be configured for each EIGRP VRF that runs between the PE and CE routers.</li> </ul>
Step 12	<b>redistribute eigrp as-number [metric metric-value] [route-map map-name]</b>  <b>Example:</b> Router(config-router-af)# redistribute eigrp 101	Redistributes the EIGRP VRF into BGP. <ul style="list-style-type: none"> <li>The autonomous system number from the CE network is configured in this step.</li> </ul>
Step 13	<b>no synchronization</b>  <b>Example:</b> Router(config-router-af)# no synchronization	Configures BGP to send advertisements without waiting to synchronize with the IGP.
Step 14	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode and enters router configuration mode.
Step 15	<b>end</b>  <b>Example:</b> 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.

#### Prerequisites

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.

#### Restrictions

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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router eigrp 1	Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> <li>The EIGRP routing process for the PE router is created in this step.</li> </ul>
Step 4	<b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 vrf RED	Enters address-family configuration mode and creates a VRF. <ul style="list-style-type: none"> <li>The VRF name must match the VRF name that was created in the previous section.</li> </ul>
Step 5	<b>network</b> <i>ip-address wildcard-mask</i>  <b>Example:</b> Router(config-router-af)# network 172.16.0.0 0.0.255.255	Specifies the network for the VRF. <ul style="list-style-type: none"> <li>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.</li> </ul>
Step 6	<b>redistribute bgp</b> { <i>as-number</i> } [ <b>metric</b> <i>bandwidth delay reliability load mtu</i> ] [ <b>route-map</b> <i>map-name</i> ]  <b>Example:</b> Router(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500	Redistributes BGP into the EIGRP. <ul style="list-style-type: none"> <li>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.</li> </ul>

	Command or Action	Purpose
Step 7	<b>autonomous-system</b> <i>as-number</i>  <b>Example:</b> Router(config-router-af)# autonomous-system 101	Specifies the autonomous system number of the EIGRP network for the customer site.
Step 8	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode and enters router configuration mode.
Step 9	<b>end</b>  <b>Example:</b> 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

---

#### Step 1 **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 27](#)
- [Verifying that the Local and Remote CE Routers are in the Routing Table, page 28](#)

## 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-number* | *access-list-name*]
5. **disable**

## 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 diagnose 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-number* | *access-list-name*]

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**

---

### 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 CEF forwarding table associated with a VRF. Check that the prefix of the remote CE router is in the CEF table.

**Step 4**    **exit**

---

## Configuration Examples for MPLS VPNs

- [Configuring an MPLS VPN Using BGP: Example, page 30](#)
- [Configuring an MPLS VPN Using RIP: Example, page 31](#)
- [Configuring an MPLS VPN Using Static Routes: Example, page 32](#)
- [Configuring an MPLS VPN Using OSPF: Example, page 33](#)
- [Configuring an MPLS VPN Using EIGRP: Example, page 34](#)

## Configuring an MPLS VPN Using BGP: Example

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

PE Configuration	CE Configuration
<pre> 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 Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router ospf 100   network 10.0.0. 0.0.0.0 area 100   network 30.0.0.0 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 34.0.0.1 remote-as 200   neighbor 34.0.0.1 activate   neighbor 34.0.0.1 as-override   neighbor 34.0.0.1 advertisement-interval 5   no auto-summary   no synchronization   exit-address-family </pre>	<pre> 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 Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router bgp 200   bgp log-neighbor-changes   neighbor 34.0.0.2 remote-as 100 ! address-family ipv4   redistribute connected   neighbor 34.0.0.2 activate   neighbor 34.0.0.2 advertisement-interval 5   no auto-summary   no synchronization   exit-address-family </pre>

## Configuring an MPLS VPN Using RIP: Example

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

PE Configuration	CE Configuration
<pre> 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 Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   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 34.0.0.0   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 </pre>	<pre> 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 Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable  router rip   version 2   timers basic 30 60 60 120   redistribute connected   network 10.0.0.0   network 34.0.0.0   no auto-summary </pre>

## Configuring an MPLS VPN Using Static Routes: Example

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

PE Configuration	CE Configuration
<pre> 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 Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 30.0.0.0 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 vpv4   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 34.0.0.1 ip route vrf vpn1 34.0.0.0 255.0.0.0 34.0.0.1 </pre>	<pre> ip cef ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! ip route 10.0.0.9 255.255.255.255 34.0.0.2 3 ip route 31.0.0.0 255.0.0.0 34.0.0.2 3 </pre>



## Configuring an MPLS VPN Using OSPF: Example

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

PE Configuration	CE Configuration
<pre> 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 Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   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 34.0.0.0 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 </pre>	<pre> 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 Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router ospf 1000   log-adjacency-changes   auto-cost reference-bandwidth 1000   redistribute connected subnets   network 34.0.0.0 0.255.255.255 area 1000   network 10.0.0.0 0.0.0.0 area 1000 </pre>

## Configuring an MPLS VPN Using EIGRP: Example

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

PE Configuration	CE Configuration
<pre> 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 Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   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 34.0.0.0   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 </pre>	<pre> 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 Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router eigrp 1000   network 34.0.0.0   auto-summary </pre>

# Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

Related Topic	Document Title
MPLS VPN Carrier Supporting Carrier	<ul style="list-style-type: none"> <li><a href="#">MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li><a href="#">MPLS VPN Carrier Supporting Carrier with BGP</a></li> </ul>
MPLS VPN InterAutonomous Systems	<ul style="list-style-type: none"> <li><a href="#">MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> <li><a href="#">MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> </ul>

## 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 IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2547	BGP/MPLS VPNs

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Feature Information for MPLS Layer 3 VPNs

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1**      **Feature Information for MPLS Layer 3 VPNs**

Feature Name	Releases	Feature Configuration Information
MPLS Virtual Private Networks	12.0(5)T 12.0(21)ST 12.0(22)S 12.0(23)S 12.2(13)T 12.2(14)S 12.0(26)S	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">MPLS VPN Definition, page 4</a></li> <li>• <a href="#">How an MPLS VPN Works, page 5</a></li> <li>• <a href="#">Major Components of MPLS VPNs, page 7</a></li> <li>• <a href="#">Benefits of an MPLS VPN, page 7</a></li> <li>• <a href="#">How to Configure MPLS Layer 3 VPNs, page 9</a></li> </ul>
MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge	12.0(22)S 12.2(15)T 12.2(18)S 12.0(27)S	<p>This feature allows you to connect customers running EIGRP to an MPLS VPN.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring EIGRP as the Routing Protocol Between the PE and CE Routers, page 23</a></li> <li>• <a href="#">Configuring EIGRP Redistribution in the MPLS VPN, page 25</a></li> </ul>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005-2008 Cisco Systems, Inc. All rights reserved

