Configuring MPLS Layer 3 VPN over GRE

- Prerequisites for MPLS Layer 3 VPN over GRE, on page 1
- Restrictions for MPLS Layer 3 VPN over GRE, on page 1
- Information About MPLS Layer 3 VPN over GRE, on page 2
- How to Configure MPLS Layer 3 VPN over GRE, on page 4
- Configuration Examples for MPLS Layer 3 VPN over GRE, on page 5
- Feature History for Configuring MPLS Layer 3 VPN over GRE, on page 11

Prerequisites for MPLS Layer 3 VPN over GRE

- Ensure that your Multiprotocol Label Switching (MPLS) virtual private network (VPN) is configured.
- Ensure that the following routing protocols are configured:
  - Label Distribution Protocol (LDP): For MPLS label distribution.
  - Multiprotocol Border Gateway Protocol (MP-BGP): For VPN route and label distribution.
- We recommend that you use the Quality of Service (QoS) group value for defining QoS policies to traverse the protocol boundary. QoS group values are required because the ingress traffic enters the IP core from the MPLS network and the egress traffic leaves the IP core to enter the MPLS network.
- Before configuring a generic routing encapsulation (GRE) tunnel, configure a loopback interface (that is not attached to a virtual routing and forwarding [VRF]) interface with an IP address. This dummy loopback interface with an IPv4 address enables the internally created tunnel interface for IPv4 forwarding. You do not have to configure a loopback interface if the system has at least one interface that is not attached to the VRF and is configured with an IPv4 address.

Restrictions for MPLS Layer 3 VPN over GRE

The MPLS Layer 3 VPN over GRE feature does not support the following:

- QoS service policies that are configured on the tunnel interface

Note Although QoS service policies configured on the tunnel interface are not supported, QoS service policies configured on a physical interface or a sub-interface are supported.

- GRE options such as sequencing, checksum, and source route
- IPv6 GRE configurations
- Advanced features such as Carrier Supporting Carrier (CSC)

Information About MPLS Layer 3 VPN over GRE

The MPLS Layer 3 VPN over GRE feature provides a mechanism for tunneling MPLS packets over non-MPLS networks. This feature 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.

Types of Tunneling Configurations

The following sections provide information about the different types of tunneling configurations that are supported.

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.

As shown in the Figure 1: PE-to-PE Tunneling, on page 3, the PE devices assign VRF numbers to the customer edge (CE) devices on each side of the non-MPLS network.

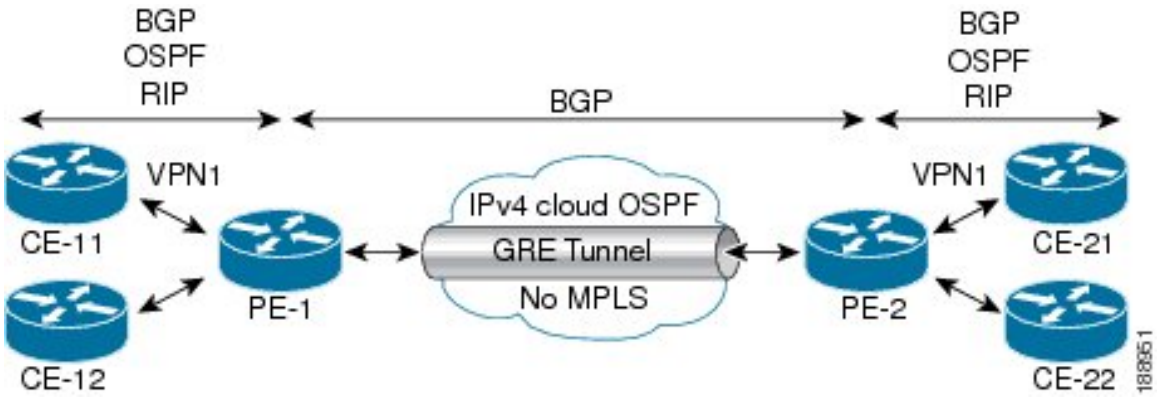
The PE devices use routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP) to learn about the IP networks behind the CE devices. The routes to the IP networks behind the CE devices are stored in the associated CE device's VRF routing table.

The PE device on one side of the non-MPLS network uses routing protocols (that operate within the non-MPLS network) to learn about the PE device on the other side of the non-MPLS network. The learned routes that are established between the PE devices are then stored in the main or default routing table.

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

Figure 1: PE-to-PE Tunneling, on page 3 shows BGP defining a static route to the BGP neighbor (the opposing PE device) 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 the customer network traffic is sent using the GRE tunnel.

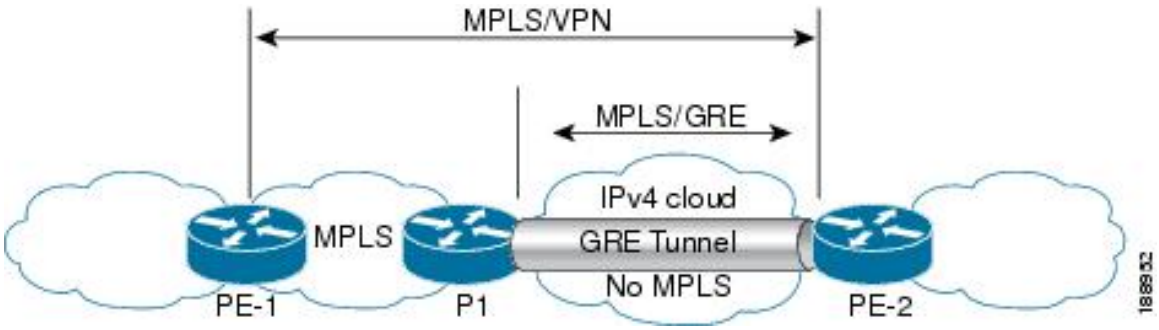
Figure 1: PE-to-PE Tunneling



P-to-PE Tunneling

Figure 2: P-to-PE Tunneling, on page 3 shows a method of connecting two MPLS segments (P2 to PE2) 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.

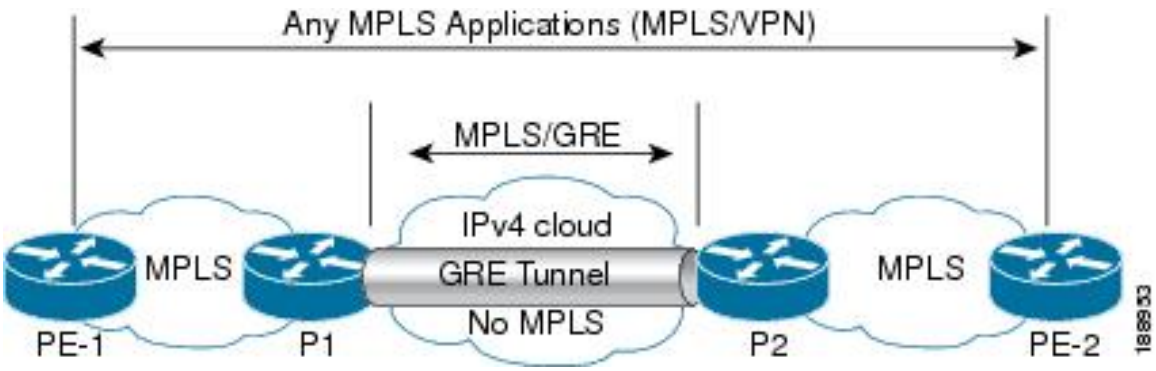
Figure 2: P-to-PE Tunneling



P-to-P Tunneling

Figure 3: P-to-P Tunneling, on page 4 shows 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 3: P-to-P Tunneling



How to Configure MPLS Layer 3 VPN over GRE

To configure the MPLS over GRE feature, you must create a GRE tunnel to span the non-MPLS networks. Perform the following procedure on the devices that are located at both ends of the GRE tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *tunnel-number* **Example:** `Device(config)# interface tunnel 1`	Creates a tunnel interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(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:** `Device(config-if)# tunnel source 10.1.1.1`	Configures the tunnel's source IP address.
Step 6	**tunnel destination** *destination-address* **Example:** `Device(config-if)# tunnel destination 10.1.1.2`	Configures the tunnel's destination IP address.

	Command or Action	Purpose
Step 7	**mpls ip** **Example:** `Device(config-if)# mpls ip`	Enables MPLS on the tunnel's physical interface.
Step 8	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for MPLS Layer 3 VPN over GRE

The following sections provide various configuration examples for MPLS Layer 3 VPN over GRE.

Example: Configuring MPLS Layer 3 VPN over GRE (PE-to-PE Tunneling)

The following examples show how to configure Layer 3 VPN and the GRE tunnel from PE1 to PE2 (see Figure 1: PE-to-PE Tunneling, on page 3).

The following example shows how to configure a loopback interface on PE1:

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback10
Device(config-if)# ip address 209.165.200.225 255.255.255.255
Device(config-if)# end
```

The following example shows how to configure a loopback interface on PE2:

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback3
Device(config-if)# ip address 209.165.202.129 255.255.255.255
Device(config-if)# end
```

The following example shows how to advertise a loopback in IGP on PE1:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 10
Device(config-router)# router-id 198.51.100.10
Device(config-router)# end
```

The following example shows how to configure a GRE tunnel, configure a different IGP instance on the tunnel, and enable MPLS on the tunnel on PE1:

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel13
Device(config-if)# ip address 203.0.113.200 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.200.225
Device(config-if)# tunnel destination 209.165.202.129
Device(config-if)# end
```

The following example shows how to configure a GRE tunnel, configure a different IGP instance on the tunnel, and enable MPLS on the tunnel on PE2:

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel31
Device(config-if)# ip address 203.0.113.201 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.202.129
Device(config-if)# tunnel destination 209.165.200.225
Device(config-if)# end
```

The following example shows how to advertise PE1 loopback IP for BGP in IGP instance configured on the tunnel:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 11
Device(config-router)# router-id 198.51.100.11
Device(config-router)# network 192.0.1.1 0.0.0.0 area 0
Device(config-router)# end
```

The following example shows how to advertise PE2 loopback IP for BGP in IGP instance configured on the tunnel:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 11
Device(config-router)# router-id 203.0.113.201
Device(config-router)# network 192.0.1.1 0.0.0.0 area 0
Device(config-router)# end
```

The following example shows how to configure VRF on PE1 where CE1 is connected:

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf-1
Device (config-vrf)# rd 1:1
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:2
Device (config-vrf-af)# route-target export 1:1
Device(config-vrf)# end
```

The following example shows how to configure VRF on PE2 where CE2 is connected:

```
Device> enable
Device# configure terminal
Device (config)# vrf definition vrf-1
Device (config-vrf)# rd 2:2
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:1
Device (config-vrf-af)# route-target export 1:2
Device(config-vrf)# end
```

The following example shows how to configure PE1-CE1 interface:

```
Device> enable
Device# configure terminal
Device (config)# int po14.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 14.2.1.1 255.255.255.0
Device(config-subif)# end
```

The following example shows how to configure PE2-CE2 interface:

```
Device> enable
Device# configure terminal
Device (config)# int po24.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 24.2.1.1 255.255.255.0
Device(config-subif)# end
```

The following example shows how to configure PE1-CE1 External Border Gateway Protocol (EBGP):

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 14.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 14.2.1.2 activate
Device (config-router-af)# exit-address-family
Device(config-router)# end
```

The following example shows how to configure PE2-CE2 EBGP:

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 24.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 24.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

The following example shows how to configure PE1-PE2 MP-BGP on PE1:

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# neighbor 192.0.2.1 remote-as 65040
Device (config-router)# neighbor 192.0.2.1 update-source Loopback0
Device (config-router)# address-family ipv4
Device (config-router-af)# neighbor 192.0.2.1 activate
Device (config-router-af)# exit
Device (config-router)# address-family vpnv4
Device (config-router-af)#  neighbor 192.0.2.1 activate
Device (config-router-af)#  neighbor 192.0.2.1 send-community both
Device (config-router-af)# exit
Device (config-router)# end
```

Example: Configuring MPLS Layer 3 VPN over GRE (P-to-PE Tunneling)

The following examples show how to configure Layer 3 VPN on the PE devices (PE1 and PE2) and MPLS segment (P1), and the GRE tunnel from PE1 to P1 to PE2 (see Figure 2: P-to-PE Tunneling, on page 3).

The following example shows how to configure loopback interface for GRE tunnel for PE1:

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback4
```

```
Device(config-if)# ip address 209.165.200.230 255.255.255.255
Device(config-if)# end
```

The following example shows how to configure loopback interface for GRE tunnel for P1:

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback100
Device(config-if)# ip address 209.165.200.235 255.255.255.255
Device(config-if)# end
```

The following example shows how to configure interface from PE1-P1 and configure IGP:

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel11
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.1 255.255.255.248
Device(config-if)# ip ospf 10 area 0
Device(config-if)# end
```

The following example shows how to configure interface from P1-PE1 and configure IGP:

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel1
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.2 255.255.255.248
Device(config-if)# ip broadcast-address 209.165.201.31
Device(config-if)# ip ospf 10 area 0
Device(config-if)# end
```

The following example shows how to advertise loopback in IGP on PE1:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 10
Device(config-router)# router-id 198.51.100.10
Device(config-router)# network 209.165.200.230 0.0.0.0 area 0
Device(config-router)# end
```

The following example shows how to advertise loopback in IGP on P1:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 10
Device(config-router)# router-id 198.51.100.20
Device(config-router)# network 209.165.200.235 0.0.0.0 area 0
Device(config-router)# end
```

The following example shows how to configure GRE tunnel, configure an IGP instance on the tunnel, and enable MPLS on the tunnel on PE1:

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel111
Device(config-if)# ip address 209.165.202.140 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.200.230
Device(config-if)# tunnel destination 209.165.200.235
Device(config-if)# end
```

The following example shows how to configure GRE tunnel, configure an IGP instance on the tunnel, and enable MPLS on the tunnel on P1:

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel111
Device(config-if)# ip address 209.165.202.141 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.200.235
Device(config-if)# tunnel destination 209.165.200.230
Device(config-if)# end
```

The following example shows how to advertise PE loopback IP for BGP in tunnel's IGP instance on PE1:

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel111
Device(config)# router ospf 11
Device(config-router)# router-id 198.51.100.11
Device(config-router)# network 192.0.1.1 0.0.0.0 area 0
Device(config-router)# end
```

The following example shows how to configure interface from PE2-P1, and configure IGP and MPLS:

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel12
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.1 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# end
```

The following example shows how to configure interface from P1-PE2, and configure IGP:

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel12
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.2 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# end
```

The following example shows how to create VRF on PE1 where CE1 is connected:

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf-1
Device (config-vrf)# rd 1:1
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:2
Device (config-vrf-af)# route-target export 1:1
Device (config-vrf-af)# exit
Device (config-vrf)# end
```

The following example shows how to create VRF on PE2 where CE2 is connected:

```
Device> enable
Device# configure terminal
Device (config)# vrf definition vrf-1
Device (config-vrf)# rd 2:2
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:1
Device (config-vrf-af)# route-target export 1:2
```

```
Device (config-vrf-af)# exit
Device (config-vrf)# end
```

The following example shows how to configure PE1-CE1 interface:

```
Device> enable
Device# configure terminal
Device (config)# int po14.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 14.2.1.1 255.255.255.0
Device (config-subif)# exit
Device (config)# end
```

The following example shows how to configure PE2-CE2 interface:

```
Device> enable
Device# configure terminal
Device (config)# int po24.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 24.2.1.1 255.255.255.0
Device (config-subif)# exit
Device (config)# end
```

The following example shows how to configure PE1-CE1 EBGP:

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 14.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 14.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

The following example shows how to configure PE2-CE2 EBGP:

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 24.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 24.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

The following example shows how to configure PE1-PE2 MP-BGP on PE1:

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# neighbor 192.0.2.1 remote-as 65040
Device (config-router)# neighbor 192.0.2.1 update-source Loopback0
Device (config-router)# address-family ipv4
Device (config-router-af)# neighbor 192.0.2.1 activate
Device (config-router-af)# exit
Device (config-router)# address-family vpnv4
Device (config-router-af)# neighbor 192.0.2.1 activate
Device (config-router-af)# neighbor 192.0.2.1 send-community both
Device (config-router-af)# exit
Device (config-router)# end
```

The following example shows how to configure PE2-PE1 MP-BGP on PE2:

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# neighbor 192.0.1.1 remote-as 65040
Device (config-router)# neighbor 192.0.1.1 update-source Loopback0
Device (config-router)# address-family ipv4
Device (config-router-af)# neighbor 192.0.1.1 activate
Device (config-router-af)# exit
Device (config-router)# address-family vpnv4
Device (config-router-af)# neighbor 192.0.1.1 activate
Device (config-router-af)# neighbor 192.0.1.1 send-community both
Device (config-router-af)# exit
Device (config-router)# end
```

Feature History for Configuring MPLS Layer 3 VPN over GRE

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.12.1	MPLS Layer 3 VPN over GRE	The MPLS Layer 3 VPN over GRE feature provides a mechanism for tunneling MPLS packets over a non-MPLS network.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/

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