MPLS VPN—L3VPN over GRE

First Published: September 29, 2008
Last Updated: September 01, 2011

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

The MPLS VPN—L3VPN over GRE feature utilizes MPLS over generic routing encapsulation (MPLSoGRE) to encapsulate MPLS packets inside IP tunnels thus creating virtual point-to-point links across non-MPLS networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for MPLS VPN—L3VPN over GRE" section on page 10.

Use Cisco Feature Navigator to find information about platform support and Cisco 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

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

Prerequisites for MPLS VPN—L3VPN over GRE

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

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

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

Restrictions for MPLS VPN—L3VPN over GRE

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

- Quality of service (QoS) service policies configured on the tunnel interface; they are supported on the physical or subinterface
- GRE options: sequencing, checksum, and source route
- IPv6 GRE
- Advanced features such as Carrier Supporting Carrier (CSC) and Interautonomous System (Inter-AS)
- For provider edge-to-provider edge (PE-to-PE) tunneling, configure tunnels with the same source and destination address.

Information About MPLS VPN—L3VPN over GRE

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

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

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

- PE-to-PE Tunneling, page 2
- P-to-PE Tunneling, page 3
- P-to-P Tunneling, page 4

PE-to-PE Tunneling

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

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

As shown in Figure 1, the PE routers assign VPN routing and forwarding (VRF) numbers to the customer edge (CE) routers on each side of the non-MPLS network.

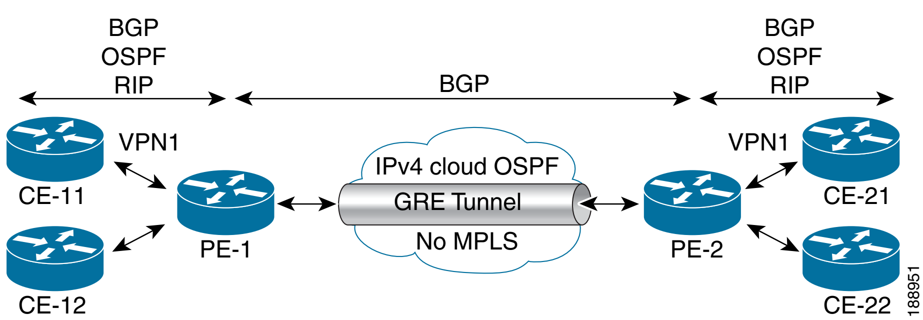
The PE routers use routing protocols such as Border Gateway Protocol (BGP), OSPF Open Shortest Path First (OSPF), or Routing Information Protocol (RIP) to learn about the IP networks behind the CE routers. The routes to the IP networks behind the CE routers are stored in the associated CE router's VRF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

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

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

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

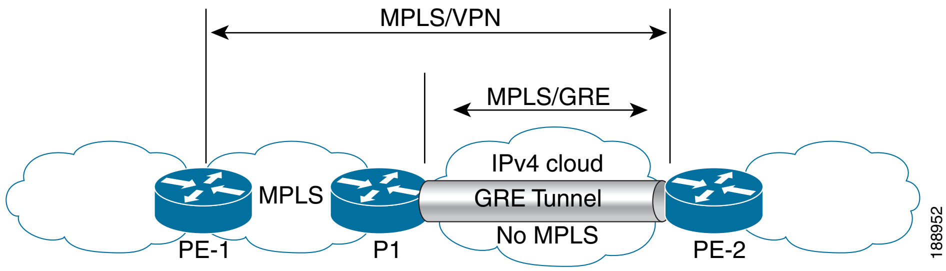
Figure 1 PE-to-PE Tunneling



P-to-PE Tunneling

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

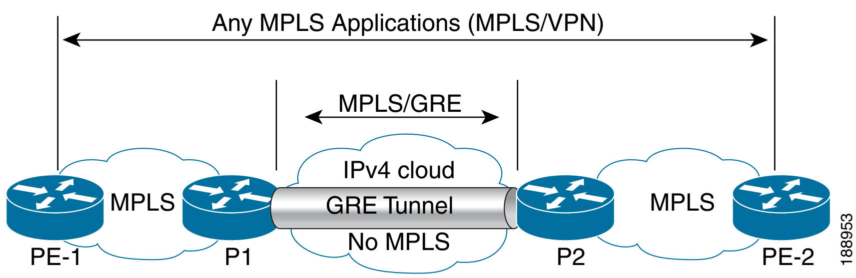
Figure 2 P-to-PE Tunneling



P-to-P Tunneling

As shown in Figure 3, the provider-to-provider (P-to-P) configuration provides a method of connecting two MPLS segments (P1 to P2) across a non-MPLS network. In this configuration, MPLS traffic that is destined to the other side of the non-MPLS network is sent through a single GRE tunnel.

Figure 3 P-to-P Tunneling



How to Configure MPLS VPN—L3VPN over GRE

- Configuring the MPLS VPN—L3VPN over GRE Tunnel Interface, page 4 (required)

Configuring the MPLS VPN—L3VPN over GRE Tunnel Interface

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

Prerequisites

Before configuring the MPLS VPN—L3VPN over GRE feature, ensure that your MPLS VPN and the appropriate routing protocols are configured and working properly. See the "Prerequisites for MPLS VPN—L3VPN over GRE" section on page 2.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
5. **tunnel source** *source-address*
6. **tunnel destination** *destination-address*
7. **mpls ip**
8. **exit**
9. **show ip route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *tunnel-number* **Example:** `Router(config)# interface tunnel 1`	Creates a tunnel on the specified interface and enters interface configuration mode.
Step 4	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*] **Example:** `Router(config-if)# ip route 209.165.200.253 255.255.255.224 FastEthernet 0/0`	Configures a static route to the BGP neighbor on the SIP 2 interface or tunnel interface.
Step 5	**tunnel source** *source-address* **Example:** `Router(config-if)# tunnel source 209.165.200.254`	Specifies the tunnel's source IP address.
Step 6	**tunnel destination** *destination-address* **Example:** `Router(config-if)# tunnel destination 209.165.200.255`	Specifies the tunnel's destination IP address.

	Command or Action	Purpose
Step 7	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS on the tunnel's physical interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**show ip route** **Example:** `Router(config)# show ip route`	Displays the current state of the routing table.

Examples

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

PE1 Configuration

```
Router# configure terminal
Router(config)# interface Tunnel 1
Router(config-if)# ip address 209.165.200.253 255.255.255.224
Router(config-if)# tunnel source 209.165.200.254
Router(config-if)# tunnel destination 209.165.200.255
Router(config-if)# mpls ip
```

PE2 Configuration

```
Router# configure terminal
Router(config)# interface Tunnel 1
Router(config-if)# ip address 209.165.200.235 255.255.255.224
Router(config-if)# tunnel source 209.165.200.240
Router(config-if)# tunnel destination 209.165.200.245
Router(config-if)# mpls ip
```

Configuration Examples for MPLS VPN—L3VPN over GRE

Example: Configuring the MPLS VPN—L3VPN over GRE Tunnel Interface

The following basic MPLS configuration example uses a GRE tunnel to span a non-MPLS network. This example is similar to the configuration shown in Figure 1 on page 3.

PE1 Configuration

```
!
```

```
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
interface loopback 0
ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet 0/1/2
ip address 209.165.200.226 255.255.255.224
!
interface Tunnel 1
ip address 209.165.200.227 255.255.255.224
tunnel source 209.165.200.228
tunnel destination 209.165.200.229
mpls ip
!
interface GigabitEthernet 0/1/3
ip vrf forwarding vpn1
ip address 209.165.200.230 255.255.255.224
!
router bgp 100
neighbor 209.165.200.231 remote-as 100
neighbor 209.165.200.231 update-source loopback0
!
address-family vpnv4
neighbor 209.165.200.232 activate
neighbor 209.165.200.232 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 209.165.200.240 remote-as 20
neighbor 209.165.200.240 activate
!
```

PE2 Configuration

```
!
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
interface loopback 0
ip address 209.165.200.240 255.255.255.224
!
interface GigabitEthernet 0/1/1
ip address 209.165.200.241 255.255.255.224
!
interface Tunnel 1
ip address 209.165.200.244 255.255.255.224
tunnel source 209.165.200.245
tunnel destination 209.165.200.247
mpls ip
!
interface GigabitEthernet 0/0/5
ip vrf forwarding vpn1
ip address 209.165.200.249 255.255.255.224
!
router bgp 100
neighbor 209.165.200.250 remote-as 100
```

```
neighbor 209.165.200.252 update-source loopback0
!
address-family vpnv4
neighbor 209.165.200.253 activate
neighbor 209.165.200.254 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 209.165.200.254 remote-as 30
neighbor 209.165.200.255 activate
```

Example: Verifying Unicast Routes

The following example shows how to display unicast routes. This display shows the next hop for the BGP neighbor depending on the selected interface.

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     209.165.200.225/32 is subnetted, 1 subnets
O       209.165.200.226 [110/3] via 209.165.200.250, 00:09:55, POS2/0/0
     209.165.200.227/32 is subnetted, 1 subnets
C       209.165.200.229 is directly connected, Loopback0
     209.165.200.230/32 is subnetted, 1 subnets
O       209.165.200.231 [110/2] via 209.165.200.232, 00:09:55, POS2/0/0
S    209.165.200.240/8 [1/0] via 209.165.200.252
     209.165.200.245/32 is subnetted, 2 subnets
S       209.165.200.247 is directly connected, POS2/0/0
O       209.165.200.248 [110/3] via 209.165.200.249, 00:09:55, POS2/0/0
C    209.165.200.254/8 is directly connected, POS2/0/0
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for MPLS VPN—L3VPN over GRE

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for MPLS VPN—L3VPN over GRE

Feature Name	Releases	Feature Information
MPLS VPN—L3VPN over GRE feature	12.0(22)S 12.2(13)T 12.0(26)S 12.2(33)SRE	The MPLS VPN—L3VPN over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network. This feature uses no new or modified commands.