



MPLS VPN—L3VPN over GRE

First Published: September 29, 2008

Last Updated: February 27, 2009

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

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

Finding Feature Information

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

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 VPN—L3VPN over GRE, page 2](#)
- [Restrictions for MPLS VPN—L3VPN over GRE, page 2](#)
- [Information About MPLS VPN—L3VPN over GRE, page 2](#)
- [How to Configure MPLS VPN—L3VPN over GRE, page 4](#)
- [Configuration Examples for MPLS VPN—L3VPN over GRE, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)
- [Feature Information for MPLS VPN—L3VPN over GRE, page 10](#)



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)

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.

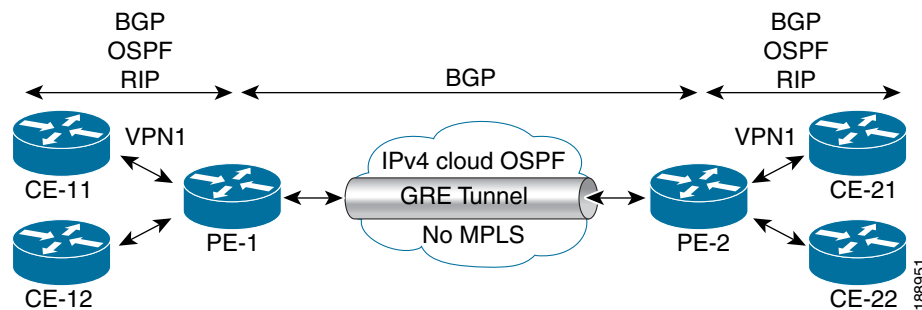
The PE routers use routing protocols such as BGP, OSPF, or Routing Information Protocol (RIP) to learn about the IP networks behind the CE routers. The routes to the IP networks behind the CE routers are stored in the associated CE router's VRF routing table.

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

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

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

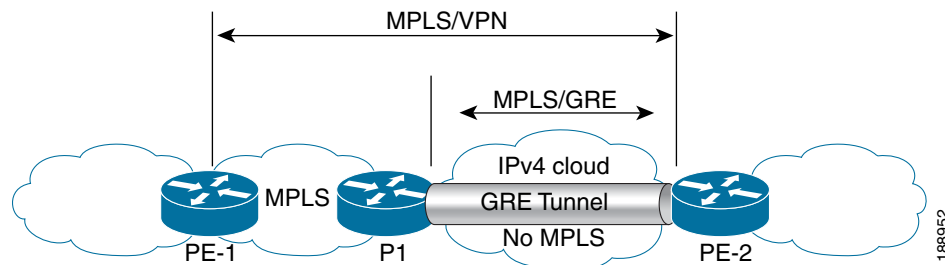
Figure 1 PE-to-PE Tunneling



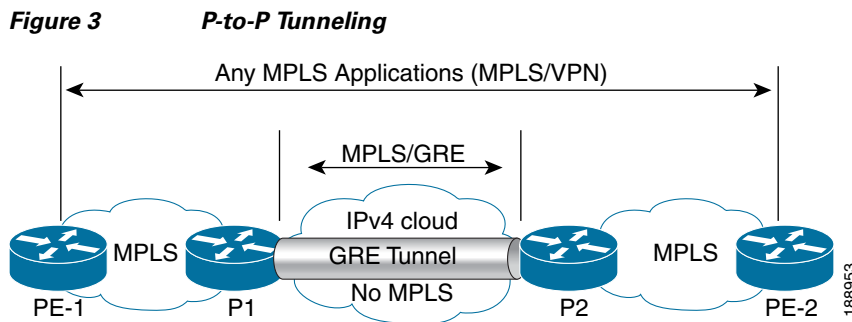
P-to-PE Tunneling

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



How to Configure MPLS VPN—L3VPN over GRE

.

Configuring the MPLS VPN—L3VPN over GRE Tunnel Interface

Prerequisites

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>tunnel-number</i> Example: Router(config)# interface tunnel 1	Creates a tunnel on the specified interface and enters interface configuration mode.
Step 4	ip address <i>ip-address</i> Example: Router(config-if)# ip address 10.0.0.1 255.255.255.0	Assigns an IP address to the tunnel interface.
Step 5	tunnel source <i>source-address</i> Example: Router(config-if)# tunnel source 10.1.1.1	Specifies the tunnel's source IP address.
Step 6	tunnel destination <i>destination-address</i> Example: Router(config-if)# tunnel destination 10.1.1.2	Specifies the tunnel's destination IP address.
Step 7	mpls ip Example: Router(config-if)# mpls ip	Enables MPLS on the tunnel's physical interface.

Examples

PE1 Configuration

```

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

```

PE2 Configuration

```

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

```

Configuration Examples for MPLS VPN—L3VPN over GRE

This section provides the following configuration example for the MPLS VPN—L3VPN over GRE feature:

- [MPLS Configuration with MPLS VPN—L3VPN over GRE: Example, page 6](#)

MPLS Configuration with MPLS VPN—L3VPN over GRE: Example

The following basic MPLS configuration example uses a GRE tunnel to span a non-MPLS network. This example is similar to the configuration shown in [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 10.2.2.2 255.255.255.255
!
interface GigabitEthernet 0/1/2
ip address 10.1.1.1 255.255.255.0
!
interface Tunnel 1
ip address 10.0.0.1 255.255.255.0
tunnel source 10.1.1.1
tunnel destination 10.1.1.2
mpls ip
!
interface GigabitEthernet 0/1/3
ip vrf forwarding vpn1
ip address 10.10.0.1 255.255.255.0
!
router bgp 100
neighbor 10.5.5.5 remote-as 100
neighbor 10.5.5.5 update-source loopback0
!
address-family vpnv4
neighbor 10.5.5.5 activate
neighbor 10.5.5.5 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 10.10.0.2 remote-as 20
neighbor 10.10.0.2 activate
!

```

PE2 Configuration

```
!  
mpls ip  
!  
ip vrf vpn1  
rd 100:1  
route-target import 100:1  
route-target export 100:1  
!  
interface loopback 0  
ip address 10.5.5.5 255.255.255.255  
!  
interface GigabitEthernet 0/1/1  
ip address 10.1.1.2 255.255.255.0  
!  
interface Tunnel 1  
ip address 10.0.0.2 255.255.255.0  
tunnel source 10.1.1.2  
tunnel destination 10.1.1.1  
mpls ip  
!  
interface GigabitEthernet 0/0/5  
ip vrf forwarding vpn1  
ip address 10.1.2.1 255.255.255.0  
!  
router bgp 100  
neighbor 10.2.2.2 remote-as 100  
neighbor 10.2.2.2 update-source loopback0  
!  
address-family vpnv4  
neighbor 10.2.2.2 activate  
neighbor 10.2.2.2 send community-extended  
!  
address-family ipv4 vrf vpn1  
neighbor 10.1.2.2 remote-as 30  
neighbor 10.1.2.2 activate  
!
```

Additional References

The following sections provide references related to the MPLS VPN—L3VPN over GRE feature.

Related Documents

Related Topic	Document Title
Setting up MPLS VPN networks	<i>Configuring MPLS Layer 3 VPNs</i>
Label Distribution Protocol	<i>MPLS Label Distribution Protocol Overview</i>
Multiprotocol Border Gateway Protocol (MP-BGP)	<i>Configuring MPLS Layer 3 VPNs</i>

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
<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>http://www.cisco.com/techsupport</p>

Command Reference

This feature uses no new or modified commands.

Feature Information for MPLS VPN—L3VPN over GRE

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 VPN—L3VPN over GRE

Feature Name	Releases	Feature Information
MPLS VPN—L3VPN over GRE feature		<p>The MPLS VPN—L3VPN over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network.</p> <p>This feature uses no new or modified commands.</p>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

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.

© 2008-2009 Cisco Systems, Inc. All rights reserved.