Configuring MPLS Traffic Engineering over GRE Tunnel Support

The MPLS Traffic Engineering (TE) over Generic Routing Encapsulation (GRE) Tunnel Support feature enables applications to establish TE tunnels over virtual interfaces.

- Prerequisites for Configuring MPLS TE over GRE Tunnel Support, on page 1
- Restrictions for Configuring MPLS TE Over GRE Tunnel Support, on page 1
- Information About Configuring MPLS TE over GRE Tunnel Support, on page 2
- How to Configure MPLS TE over GRE Tunnel Support, on page 3
- Configuration Examples for MPLS TE Over GRE Tunnel Support, on page 8
- Additional References for MPLS TE Over GRE Tunnel Support, on page 12
- Feature Information for MPLS TE Over GRE Tunnel Support, on page 13

Prerequisites for Configuring MPLS TE over GRE Tunnel Support

Your network must support the following:

- Cisco Express Forwarding
- External data encryptors
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)
- IPsec that is enabled on the GRE nodes to implement GRE traffic encryption
- MPLS TE that is configured on the interface and on GRE tunnels
- MPLS TE tunnels

If GRE tunnels and TE tunnels coexist within the same routing domain, routing loops will occur. Create separate routing domains by either configuring GRE overlay with static routing for GRE packets or using two separate routing processes, one for the GRE overlay and another for TE tunnels.

Restrictions for Configuring MPLS TE Over GRE Tunnel Support

The following TE features are not supported over GRE tunnels, so they should not be configured for TE tunnels that may traverse GRE tunnels:

- The following TE features are not supported over GRE tunnels. They should not be configured for TE tunnels that may traverse GRE tunnels:
  - Autoroute destinations
  - Automatic bandwidth adjustment
  - Autotunnel primary one-hop tunnels
  - Diff-Serve Aware TE (DS-TE)
  - Explicit path options that identify excluded nodes
  - Interarea/autonomous systems MPLS TE
  - Point-to-multipoint TE
  - Shared Risk Link Groups (SRLGs)
  - Tunnel-Based Admission Control (TBAC)
- GRE tunnels do not support Cisco nonstop forwarding with stateful switchover (NSF with SSO). If a switchover occurs, traffic loss occurs for TE over GRE, and the TE tunnels are resignaled.
- Fast Reroute (FRR) is not supported.

Information About Configuring MPLS TE over GRE Tunnel Support

MPLS TE over GRE Tunnel Support Overview

MPLS TE tunnels provide transport for label switching data through an MPLS network using a path, which is constraint-based, and is not restricted to the IGP shortest cost path. The TE tunnels are usually established over physical links between adjacent routers. However, some applications require establishing TE tunnels over virtual interfaces such as GRE tunnels. Federal Information Processing Standard (FIPS) 140-2 compliance mandates that federal customers require traffic encryption throughout their network infrastructure, which is referred to as Type-I encryption level of security. Type-I encryption environments differentiate between encrypted and unencrypted networks. The encrypted network is the secure part of the network that is in a secure facility, where encryption is not required. The unencrypted network is the unsecured part of the network where traffic encryption is required.

Two common methods of traffic encryption are as follows:

- External crypto devices
- Cisco IOS IPsec, which is the encryption embedded into Cisco IOS software

External crypto devices operate in Layer 2 (L2), providing link layer encryption of ATM and SONET traffic. Due to the migration of L2 networks to IP network, there is an increasing adoption of IP crypto devices and IPsec. This transition requires that the traffic encryption happens at the IP layer. The IP-based forwarding of service traffic, such as IP or Layer 3 (L3)/L2 VPN MPLS traffic, is implemented only through GRE tunnels.

The following MPLS TE features are supported when enabled over GRE tunnel:

- MPLS TE over GRE (Tunnel establishment and data traffic)
- Metrics (admin weight)
- Attribute flag and affinities
- Explicit path
- BFD
- ECMP without Class Based Tunnel Selection (CBTS)

Benefits of MPLS TE over GRE Tunnel Support

The MPLS TE Over GRE Tunnel Support feature enables you to leverage MPLS segmentation capabilities, such as Layer 2 and Layer 3 VPN, on GRE tunnel transport. This feature enables you to deploy MPLS TE to implement explicit path forwarding, FRR, and bandwidth management of traffic over GRE tunnels. Also, this feature helps maintain the TE capabilities currently supported by ATM legacy networks.

How to Configure MPLS TE over GRE Tunnel Support

Configuring Resource Reservation Protocol Bandwidth

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bandwidth** *kbps*
5. **ip address** *ip-address mask*
6. **mpls traffic-eng tunnels**
7. **tunnel source** *type number*
8. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
9. **ip rsvp bandwidth**
10. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type* *number* **Example:** `Router(config)# interface tunnel 0`	Configures a tunnel interface and enters interface configuration mode for the specified tunnel interface.
Step 4	**bandwidth** *kbps* **Example:** `Router(config-if)# bandwidth 100000`	Sets the total bandwidth for a bandwidth pool.
Step 5	**ip address** *ip-address* *mask* **Example:** `Router(config-if)# ip address 172.16.0.0 255.255.255.254`	Configures a primary IP address for an interface.
Step 6	**mpls traffic-eng tunnels** **Example:** `Router(config-if)# mpls traffic-eng tunnels`	Enables traffic engineering tunnel signaling on the interface.
Step 7	**tunnel source** *type* *number* **Example:** `Router(config-if)# tunnel source loopback 1`	Configures the source address for the tunnel interface.
Step 8	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} **Example:** `Router(config-if)# tunnel destination 192.168.1.1`	Specifies the destination for a tunnel. • *ip-address*—IP address of the host destination expressed in dotted decimal notation.
Step 9	**ip rsvp bandwidth** **Example:** `Router(config-if)# ip rsvp bandwidth`	Enables Resource Reservation Protocol (RSVP) for IP on an interface.
Step 10	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuring an MPLS TE Tunnel

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *tunnel* *number*
4. **ip unnumbered** *type* *number*
5. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
6. **mpls traffic-eng tunnels**
7. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
8. **tunnel mpls traffic-eng bandwidth** *kbps*
9. **tunnel mpls traffic-eng path-option** *number* **dynamic**
10. **tunnel mpls traffic-eng fast-reroute**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *tunnel* *number* **Example:** `Router(config)# interface tunnel 10`	Configures a tunnel interface and enters interface configuration mode for the specified tunnel interface.
Step 4	**ip unnumbered** *type* *number* **Example:** `Router(config-if)# ip unnumbered loopback 0`	Assigns an IP address to the tunnel interface. • An MPLS TE tunnel interface should be unnumbered because it represents a unidirectional link.
Step 5	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} **Example:** `Router(config-if)# tunnel destination 192.168.2.2`	Specifies the destination for a tunnel. • *ip-address*—IP address of the host destination expressed in dotted decimal notation.
Step 6	**mpls traffic-eng tunnels** **Example:**	Enables traffic engineering tunnel signaling on the interface.

	Command or Action	Purpose
	`Router(config-if)# mpls traffic-eng tunnels`	
Step 7	**tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*] **Example:** `Router(config-if)# tunnel mpls traffic-eng priority 7 7`	Configures the setup and reservation priority for the tunnel.
Step 8	**tunnel mpls traffic-eng bandwidth** *kbps* **Example:** `Router(config-if)# tunnel mpls traffic-eng bandwidth 10`	Configures the bandwidth required for the tunnel.
Step 9	**tunnel mpls traffic-eng path-option** *number* **dynamic** **Example:** `Router(config-if)# tunnel mpls traffic-eng path-option 10 dynamic`	Configures the path option for the tunnel.
Step 10	**tunnel mpls traffic-eng fast-reroute** **Example:** `Router(config-if)# tunnel mpls traffic-eng fast-reroute`	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.
Step 11	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuring an MPLS TE Tunnel over GRE

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *tunnel* **number**
4. **ip unnumbered loopback** *number*
5. **tunnel destination** *ip-address*
6. **tunnel mpls traffic-eng autoroute announce**
7. **tunnel mpls traffic-eng**
8. **tunnel mpls traffic-eng path-option** *number* **dynamic**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *tunnel* **number** **Example:** `Router(config)# interface tunnel 100`	Configures an interface type and enters interface configuration mode
Step 4	**ip unnumbered loopback** *number* **Example:** `Router(config-if)# ip unnumbered loopback 0`	Assigns an IP address to the tunnel interface. • An MPLS TE tunnel interface should be unnumbered because it represents a unidirectional link.
Step 5	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 10.255.1.2`	Specifies the destination for a tunnel. • *ip-address*—IP address of the host destination expressed in dotted decimal notation.
Step 6	**tunnel mpls traffic-eng autoroute announce** **Example:** `Router(config-if)# tunnel mpls traffic-eng autoroute announce`	Specifies that the IGP should use the tunnel in its enhanced shortest path first (SPF) calculation.
Step 7	**tunnel mpls traffic-eng** **Example:** `Router(config-if)# tunnel mpls traffic-eng`	Sets the encapsulation mode of the tunnel to MPLS TE.
Step 8	**tunnel mpls traffic-eng path-option** *number* **dynamic** **Example:** `Router(config-if)# tunnel mpls traffic-eng path-option 10 dynamic`	Configures a path option for the MPLS TE tunnel. • If you specify the **dynamic** keyword, the Cisco IOS software checks both the physical bandwidth of the interface and the available TE bandwidth to make sure that the requested amount of bandwidth does not exceed the physical bandwidth of any link.
Step 9	**end** **Example:**	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-if)# end	

Configuration Examples for MPLS TE Over GRE Tunnel Support

Example Configuring MPLS TE Over GRE Tunnel Support

The following example shows how to configure MPLS TE over a GRE tunnel between two routers: Router 1 and Router 2. The first loopback interface is used for router identification, and the other for reachability. One OSPF is used for TE and the other for reachability.

Router 1

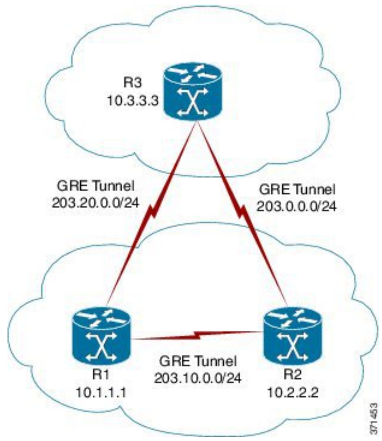
```
configure terminal
no logging console
mpls traffic-eng tunnels
interface Loopback 0
 ip address 172.16.1.1 255.255.255.255
 no shutdown
!
interface Loopback 1
 ip address 10.255.1.1 255.255.255.0
 no shutdown
!
interface gigabitethernet 1/1
 ip address 172.16.1.1 255.255.255.255
 ip rsvp bandwidth 100000
 no shutdown
!
router ospf 172
 router-id 172.16.1.1
 network 172.16.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback 0
 mpls traffic-eng area 0
 no shutdown
!
router ospf 10
 router-id 10.255.1.1
 network 10.255.0.0 0.0.255.255 area 0
 no shutdown
!
interface Tunnel 10
bandwidth 20000
 ip address 172.16.0.1 255.255.255.252
 mpls traffic-eng tunnels
 keepalive 10 3
 tunnel source Loopback 1
 tunnel destination 10.255.1.2
 ip rsvp bandwidth 15000 sub-pool 5000
!
!
interface tunnel 100
ip unnumbered loopback 0
tunnel mode mpls traffic-eng
tunnel destination 192.168.10.10
```

```
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 dynamic
!
end
Router 2
configure terminal
no logging console
mpls traffic-eng tunnels
interface Loopback 0
 ip address 172.16.1.2 255.255.255.255
 no shutdown
!
interface Loopback 1
 ip address 10.255.1.2 255.255.255.255
 no shutdown
!
interface gigabitethernet 1/1
 ip address 10.255.0.2 255.255.255.252
 ip rsvp bandwidth 100000
 no shutdown
!
router ospf 172
 router-id 172.16.1.2
 network 172.16.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback 0
 mpls traffic-eng area 0
 no shutdown
!
router ospf 10
 router-id 10.255.1.2
 network 10.255.0.0 0.0.255.255 area 0
 no shutdown
!
!
interface Tunnel0
bandwidth 20000
 ip address 172.16.0.2 255.255.255.252
 mpls traffic-eng tunnels
 keepalive 10 3
 tunnel source Loopback 1
 tunnel destination 10.255.1.1
 ip rsvp bandwidth 15000 sub-pool 5000
!
!
interface tunnel 100
ip unnumbered loopback 0
tunnel mode mpls traffic-eng
tunnel destination 172.16.1.1
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 dynamic
!
end
```

Example Configuring CBTS with MPLS over GRE

The following example shows how to configure Class-Based Tunnel Selection (CBTS) with MPLS Traffic Engineering (TE) over GRE.

Figure 1: The Network Structure of CBTS with MPLS over GRE



Configuration of the Midpoint Router (R1)

```
mpls traffic-eng tunnels
!
interface Tunnel 102
ip address 203.20.0.1 255.255.255.0
mpls ip
mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.0.1
tunnel key 22
tunnel checksum
ip rsvp bandwidth 500000
!
interface Tunnel 103
ip address 203.10.0.1 255.255.255.0
mpls ip
mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.10.1
tunnel key 33
tunnel checksum
ip rsvp bandwidth 500000
mpls traffic-eng tunnels
!
router ospf 1
router-id 10.1.1.1
network 10.1.1.1 0.0.0.0 area 1
network 203.20.0.1 0.0.0.0 area 1
network 203.10.0.1 0.0.0.0 area 1
mpls traffic-eng router-id Loopback 0
mpls traffic-eng area 1
```

Configuration of the Head Router (R2)

```
mpls traffic-eng tunnels
!
interface Tunnel 203
 ip address 203.0.0.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
```

```
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.10.1
 tunnel key 6
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 211
 ip address 172.16.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.20.1
 tunnel key 22
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 2300
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel 2301
 tunnel mpls traffic-eng exp-bundle member Tunnel 2302
!
interface Tunnel 2301
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 explicit name TE2301
 tunnel mpls traffic-eng exp 6 7
!
interface Tunnel 2302
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 explicit name TE2302
 tunnel mpls traffic-eng exp default
!
router ospf 1
 router-id 10.2.2.2
 network 10.2.2.2 0.0.0.0 area 1
 network 203.20.0.2 0.0.0.0 area 1
 network 172.16.0.2 0.0.0.0 area 1
 network 203.0.0.1 0.0.0.0 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
!
ip explicit-path name TE2301 enable
 next-address 203.0.0.2
ip explicit-path name TE2302 enable
 next-address 172.16.0.1
```

```
 next-address 172.26.0.2
```

Configuration of the Tail Router (R3)

```
mpls traffic-eng tunnels
!
interface Tunnel 302
 ip address 203.0.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.0.1
 tunnel key 6
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 311
 ip address 172.26.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.20.1
 tunnel key 33
 tunnel checksum
 ip rsvp bandwidth 500000
 !
router ospf 1
 router-id 10.3.3.3
 network 10.3.3.3 0.0.0.0 area 1
 network 203.10.0.2 0.0.0.0 area 1
 network 172.26.0.2 0.0.0.0 area 1
 network 203.0.0.2 0.0.0.0 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
!
```

Additional References for MPLS TE Over GRE Tunnel Support

Related Documents

Related Topic	Document Title
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference

Standards

Standard	Title
FIPS 140-2	Security Requirements for Cryptographic Modules.

MIBs

MIB	MIBs Link
MPLS-TE-STD-MIB	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
RFC 3812	MPLS TE Management Information Base (MIB)

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 TE Over GRE Tunnel Support

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

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

Table 1: Feature Information for MPLS TE over GRE Tunnel Support

Feature Name	Releases	Feature Information
MPLS TE over GRE Tunnel Support	Cisco IOS XE Release 3.3S 15.2(1)T Cisco IOS XE Release 3.12S Cisco IOS XE Release 3.16S	The MPLS TE over GRE Tunnel Support feature enables applications to establish traffic engineering tunnels over virtual interfaces. The following commands were introduced or modified: **mpls traffic-eng tunnels**, **tunnel mpls traffic-eng autoroute announce**. **tunnel mpls traffic-eng bandwidth**, **tunnel mpls traffic-eng fast-reroute**, **tunnel mpls traffic-eng path-option**, **tunnel mpls traffic-eng priority**. In Cisco IOS XE 3.12S release, CBTS support was added for GRE interface type on the Cisco ASR 1000 Series Aggregation Services Routers. In Cisco IOS XE 3.16S release,CBTS support was added for GRE interface type on Cisco ISR4451/4431/4351 series Integrated Services Routers.