



GRE IPv6 Tunnels

The GRE IPv6 Tunnels feature enables the delivery of packets from other protocols through an IPv6 network and allows the routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses. Generic routing encapsulation (GRE) is a unicast protocol that offers the advantages of encapsulating broadcast and multicast traffic (multicast streaming or routing protocols) or other non-IP protocols and of being protected by IPsec.

- [Finding Feature Information, page 1](#)
- [Restrictions for GRE IPv6 Tunnels, page 1](#)
- [Information About GRE IPv6 Tunnels, page 2](#)
- [How to Configure GRE IPv6 Tunnels, page 3](#)
- [Configuration Examples for GRE IPv6 Tunnels, page 6](#)
- [Additional References, page 6](#)
- [Feature Information for GRE IPv6 Tunnels, page 7](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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.

Restrictions for GRE IPv6 Tunnels

- GRE tunnel keepalive packets are not supported.
- Multipoint GRE (mGRE) IPv6 tunneling is not supported.
- There is limited support for tunnel transport in virtual routing and forwarding (VRF). The limited support in VRF is applicable to IPv6 point-to-point GRE without tunnel protection.

Information About GRE IPv6 Tunnels

Overview of GRE IPv6 Tunnels

The GRE IPv6 Tunnels feature enables the delivery of packets from other protocols through an IPv6 network and allows the routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses.

For point-to-point GRE tunnels, each tunnel interface requires a tunnel source IPv6 address and a tunnel destination IPv6 address when being configured. All packets are encapsulated with an outer IPv6 header and a GRE header.

GRE IPv6 Tunnel Protection

GRE IPv6 tunnel protection allows devices to work as security gateways, establish IPsec tunnels between other security gateway devices, and provide crypto IPsec protection for traffic from internal networks when the traffic is sent across the public IPv6 Internet. The GRE IPv6 tunnel protection functionality is similar to the security gateway model that uses GRE IPv4 tunnel protection.

Distributed GRE Tunneling Support

Distributed GRE Tunneling allows Cisco IOS software to switch packets into and out of the Generic Routing Encapsulation (GRE) tunnels using distributed Cisco Express Forwarding (dCEF). The tunneling is performed using recursive or "double" switching techniques that are currently deployed on existing non-distributed platforms. The relevant bits are ported into this development.

Double switching is performed by the handling of the received IP packet in the existing code path until it is determined that the packet needs encapsulation or de-encapsulation. Recursively forwarding the IP packet through the IP switching path again explains the "double" aspect of the switching.

The GRE tunneling allows service providers to support a large number of tunnels by forwarding distributed tunneled packets. This feature is an extension of the non-distributed forwarding information base (FIB) forwarding paths.

**Note**

dCEF must be explicitly enabled on the device before GRE tunneling. At the tunnel exit point, dCEF and Cisco Express Forwarding (CEF) GRE tunnels do not support reassembly of fragmented packets. Also, dCEF and CEF GRE tunnels do not support packet sequencing or check summing as defined in RFC 1721.

How to Configure GRE IPv6 Tunnels

Configuring GRE IPv6 Tunnels

Perform this task to configure a GRE tunnel on an IPv6 network. GRE tunnels can be configured to run over an IPv6 network layer and transport IPv6 and IPv4 packets through IPv6 tunnels.

Before You Begin

When GRE IPv6 tunnels are configured, IPv6 addresses are assigned to the tunnel source and the tunnel destination. The tunnel interface can have either IPv4 or IPv6 addresses (this is not shown in the task below). The host or device at each end of the configured tunnel must support both IPv4 and IPv6 protocol stacks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *tunnel-number***
4. **tunnel source {*ipv6-address* | *interface-type interface-number*}**
5. **tunnel destination *ipv6-address***
6. **tunnel mode gre ipv6**
7. **end**

DETAILED STEPS

	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 <i>tunnel-number</i> Example: Device(config)# interface tunnel 0	Specifies a tunnel interface and number and enters interface configuration mode.
Step 4	tunnel source {<i>ipv6-address</i> <i>interface-type interface-number</i>}	Specifies the source IPv6 address or the source interface type and number for the tunnel interface.

	Command or Action	Purpose
	Example: Device(config-if)# tunnel source ethernet 0	<ul style="list-style-type: none"> If an interface type and number are specified, the interface must be configured with an IPv6 address. Note Only the syntax used in this context is displayed. For more details, see the IPv6 Command Reference .
Step 5	tunnel destination <i>ipv6-address</i> Example: Device(config-if)# tunnel destination 2001:0DB8:0C18:2::300	Specifies the destination IPv6 address for the tunnel interface. Note Only the syntax used in this context is displayed. For more details, see the IPv6 Command Reference .
Step 6	tunnel mode <i>gre ipv6</i> Example: Device(config-if)# tunnel mode gre ipv6	Specifies a GRE IPv6 tunnel. Note The tunnel mode gre ipv6 command specifies GRE as the encapsulation protocol for the tunnel interface. Only the syntax used in this context is displayed. For more details, see the IPv6 Command Reference .
Step 7	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring GRE IPv6 Tunnel Protection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **tunnel source** *{ipv6-address | interface-type interface-number}*
5. **tunnel destination** *ipv6-address*
6. **tunnel mode** *gre ipv6*
7. **tunnel protection ipsec profile** *profile-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example: Device> enable</p>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Device# configure terminal</p>	Enters global configuration mode.
Step 3	<p>interface tunnel <i>tunnel-number</i></p> <p>Example: Device(config)# interface tunnel 0</p>	Specifies a tunnel interface and number and enters interface configuration mode.
Step 4	<p>tunnel source {<i>ipv6-address</i> <i>interface-type interface-number</i>}</p> <p>Example: Device(config-if)# tunnel source ethernet 0</p>	<p>Specifies the source IPv6 address or the source interface type and number for the tunnel interface.</p> <ul style="list-style-type: none"> • If an interface type and number are specified, the interface must be configured with an IPv6 address. <p>Note Only the syntax used in this context is displayed. For more details, see the IPv6 Command Reference.</p>
Step 5	<p>tunnel destination <i>ipv6-address</i></p> <p>Example: Device(config-if)# tunnel destination 2001:0DB8:0C18:2::300</p>	<p>Specifies the destination IPv6 address for the tunnel interface.</p> <p>Note Only the syntax used in this context is displayed. For more details, see the IPv6 Command Reference.</p>
Step 6	<p>tunnel mode gre ipv6</p> <p>Example: Device(config-if)# tunnel mode gre ipv6</p>	<p>Specifies a GRE IPv6 tunnel.</p> <p>Note The tunnel mode gre ipv6 command specifies GRE as the encapsulation protocol for the tunnel interface. Only the syntax used in this context is displayed. For more details, see the IPv6 Command Reference.</p>
Step 7	<p>tunnel protection ipsec profile <i>profile-name</i></p> <p>Example: Device(config-if)# tunnel protection ipsec profile ipsec-profile</p>	<p>Associates the tunnel interface with an IPsec profile.</p> <p>Note For the <i>profile-name</i> argument, specify the IPsec profile configured in global configuration mode.</p>
Step 8	<p>end</p> <p>Example: Device(config-if)# end</p>	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for GRE IPv6 Tunnels

Example: Configuring GRE IPv6 Tunnels

The following example shows how to configure a GRE tunnel over an IPv6 transport. In this example, Ethernet0/0 has an IPv6 address, and this is the source address used by the tunnel interface. The destination IPv6 address of the tunnel is specified directly. In this example, the tunnel carries both IPv4 and IS-IS traffic.

```
interface Tunnel0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
 tunnel source Ethernet0/0
 tunnel destination 2001:DB8:1111:2222::1
 tunnel mode gre ipv6
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001:DB8:1111:1111::1/64
!
router isis
 net 49.0001.0000.0000.000a.00
```

Example: Configuring GRE IPv6 Tunnel Protection

The following example shows how to associate the IPsec profile “ipsec-profile” with a GRE IPv6 tunnel interface. The IPsec profile is configured using the **crypto ipsec profile** command.

```
crypto ipsec profile ipsec-profile
 set transform-set ipsec-profile
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source FastEthernet2/0
 tunnel destination 10.13.7.67
 tunnel protection ipsec profile ipsec-profile
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
Tunnel commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	Interface and Hardware Component Command Reference
IPv6 commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	IPv6 Command Reference

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 GRE IPv6 Tunnels

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 GRE IPv6 Tunnels

Feature Name	Releases	Feature Information
GRE IPv6 Tunnels	Cisco IOS XE Release 3.7S 15.1(2)SY	The GRE IPv6 Tunnels feature enables the delivery of packets from other protocols through an IPv6 network and allows the routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses.

