Configuring GRE IPv6 Tunnels

Restrictions for GRE IPv6 Tunnels

- This feature is not supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
- Keepalive is not supported over GRE IPv6 Tunnels, whereas it is supported over GRE IPv4 Tunnels.
- ISIS is not supported over GRE tunnels.
- Checksum is supported over GRE IPv6 Tunnels but not over GRE IPv4 Tunnels.
- MPLS over GRE IPv6 Tunnel is not supported whereas GRE IPv6 Tunnel over MPLS is supported.
- No feature interactions such as IPSec, ACL, Tunnel counters, Crypto support, Fragmentation, Cisco Discovery Protocol (CDP), QoS, GRE keepalive, etc. are supported on GRE tunnels.

Information About GRE IPv6 Tunnels

Overview of GRE IPv6 Tunnels

Note This feature is not supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.

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.

Note You must enable IPv6 or configure IPv6 MTU size more than 1500 on a tunnel's exit interface to avoid receiving warning messages.

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. The host or device at each end of the configured tunnel must support both IPv4 and IPv6 protocol stacks.

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 0`	Specifies a tunnel interface and number and enters interface configuration mode.

Step 4	**tunnel source** {*ipv6-address* | *interface-type* |*interface-number* }
	Example:
	`Device(config-if)# tunnel source ethernet 0`
		Specifies the source IPv6 address or the source interface type and number for the tunnel interface.
		• If an interface type and number are specified, the interface must be configured with an IPv6 address.
		Note For more information on the tunnel source command, refer to the IPv6 command reference guide.

Step 5	**tunnel destination** *ipv6-address* **Example:** `Device(config-if)# tunnel destination 2001:0DB8:0C18:2::300`	Specifies the destination IPv6 address for the tunnel interface. **Note** For more information on the tunnel destination command, refer to the IPv6 command reference guide.
Step 6	**tunnel mode gre ipv6** **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.

	Command or Action	Purpose

Step 7	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring GRE IPv6 Tunnel Protection

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 0`	Specifies a tunnel interface and number and enters interface configuration mode.

Step 4	**tunnel source** {*ipv6-address* | *interface-type interface-number*}
	Example:
	`Device(config-if)# tunnel source ethernet 0`
		Specifies the source IPv6 address or the source interface type and number for the tunnel interface.
		• 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** *ipv6-address* **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 gre ipv6** **Example:**	Specifies a GRE IPv6 tunnel.

	Command or Action	Purpose
	`Device(config-if)# tunnel mode gre ipv6`	**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	**tunnel protection ipsec profile** *profile-name* **Example:** `Device(config-if)# tunnel protection ipsec profile ipsec-profile`	Associates the tunnel interface with an IPsec profile. **Note** For the *profile-name* argument, specify the IPsec profile configured in global configuration mode.

Step 8	**end**
	Example:
	`Device(config-if)# end`
		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
```