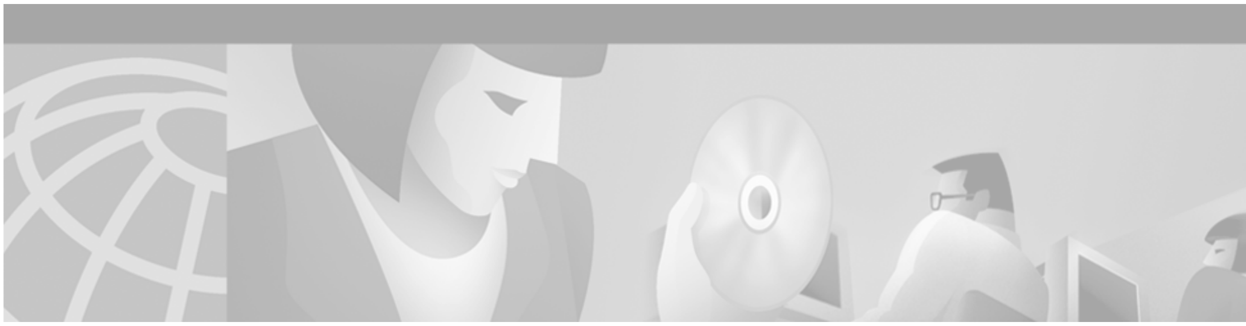


GRE Tunneling on Cisco 12000 Series Internet Routers

Feature History

Release	Modification
12.0(21)S	The GRE Tunneling feature was introduced on Cisco 12000 series Internet routers.

This feature module describes the Generic Routing Encapsulation (GRE) Tunneling feature and how it is implemented in Cisco 12000 series Internet routers. This document includes the following sections:

Feature Overview

The GRE Tunneling feature allows you to create a virtual point-to-point link to transmit packets between routers at remote distances over an IP network.

GRE Tunneling Protocol

GRE is a standards-based tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP network. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

Note In Cisco 12000 series Internet routers, only IP over GRE tunneling is supported.

Figure 1 GRE Tunneling Between Provider Edge Routers

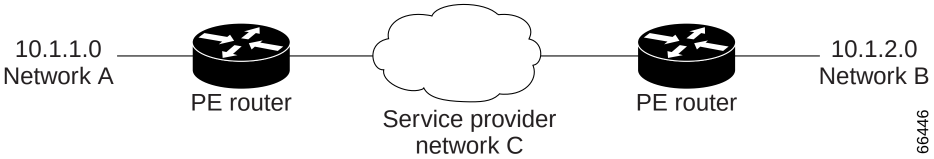


Figure 1 shows a high-level view of a GRE tunnel in a service provider network. Traffic from device 10.1.1.0 in network A is sent through the provider network C to device 10.1.2.0 in network B. GRE tunneling allows networks A and B to appear to be directly connected. The only knowledge that the provider network has of the two customer networks is at the interfaces of the provider edge (PE) routers.

One way to set up the virtual link between networks A and B is to encapsulate traffic from 10.1.1.0 in a GRE IP packet with a source and destination address that network C recognizes. If the source address of the packet is the PE router at the ingress point from network A, and the destination address is the router that injects the packet into network B, all traffic sent from network A to network B can be transmitted across network C, without network C's internal routers knowing anything about network A and network B. The entire encapsulated packet is shown in Figure 2.

Figure 2 GRE Encapsulated Packet Structure

Carrier IP Header
GRE Header
Payload IP Header

Implementing GRE Tunneling on Cisco 12000 Series Internet Routers

This section describes how GRE tunneling is implemented on Cisco 12000 series Internet routers, including:

- GRE header format
- Tunnel server card
- GRE packet processing

GRE Header Format

In the implementation of GRE tunneling on Cisco 12000 series Internet routers, a fixed 4-byte header is used as shown in Figure 3. The Flags and Version fields are set to all zeros. Only IP is supported as a payload protocol. The protocol type for IP is 0x0800. Therefore, the value of the 4-byte GRE header must always be 0x00000800.

Figure 3 GRE Header Format Supported on the Cisco 12000 Series Internet Router

Flags + Version (two bytes)	Protocol Type (two bytes)

Tunnel Server Card

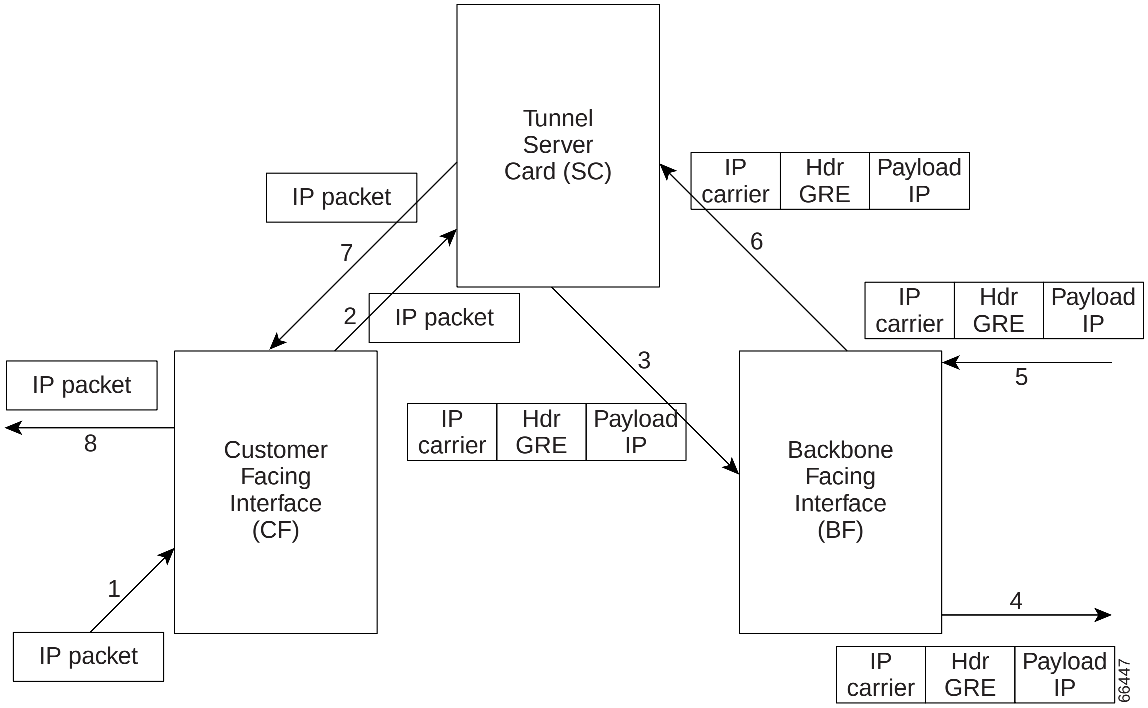
GRE tunneling is enabled on the Cisco 12000 series Internet router using a tunnel server card. The tunnel server card is an Enhanced OC-48c/STM-16c Packet-Over-SONET (POS) line card with a new software image.

All traffic destined to a GRE tunnel and GRE traffic terminating on the router is sent from the ingress line card to the tunnel server card. Approximately 2.7 Mpps of GRE tunneling traffic per router is provided regardless of what types of line cards are installed in the router. Features such as ACLs and CAR are not supported on the tunnel interface or on traffic traversing the tunnel server card.

GRE Packet Processing

GRE packet processing on the Cisco 12000 series Internet router is designed to support as many line cards as possible with the highest forwarding rate. The dedicated tunnel server card performs all GRE tunnel encapsulation and decapsulation.

Figure 4 GRE Packet Flow in the Cisco 12000 Series Internet Router



GRE Tunnel Encapsulation and Decapsulation

In Figure 4, the traffic flows numbered 1 to 4 show how GRE tunneling encapsulates incoming IP packets:

Step 1 A packet arrives on a customer-facing interface and an IP destination lookup is performed. When a packet needs to pass through a GRE tunnel, the next hop of the packet is the tunnel server card.

Step 2 The packet is routed to the tunnel server card.

Step 3 The tunnel server card adds the carrier IP header and GRE header. The packet is then transmitted out of the tunnel server card and looped back into the receiving side. Then the packet is forwarded as a normal IP packet to the appropriate egress interface.

Step 4 The egress interface sends the packet out on the wire. The TTL value of the carrier IP header is provisioned from the command line interface.

You can optionally configure the ToS bits of the tunnel (for example, the carrier IP header). If you do not configure the tunnel ToS, by default the ToS value of the carrier IP header is copied from the corresponding ToS bits of the passenger IP header.

In Figure 4, the traffic flows numbered 5 to 8 show how GRE tunneling decapsulates IP packets received from the provider network:

Step 5 The packet arrives on the terminating router and a lookup is made on the destination IP address.

Step 6 For GRE packets, the lookup indicates that the next hop for the packet uses the tunnel server card. The packet is sent to the tunnel server card.

Step 7 The tunnel server card checks the packet against the corresponding GRE tunnel record. If the check succeeds, an IP lookup is performed on the IP destination of the underlying packet and appropriate statistics are updated. Then the carrier IP header and GRE header are stripped off, and the underlying packet is routed to the egress card.

Step 8 The egress card sends the passenger IP packet out on the wire.

Exception Behavior

For GRE packets destined to a Cisco 12000 Internet series router used as an edge router with GRE tunneling, exception behavior is handled in the following ways:

- If the payload for the GRE packet is destined for the router, the packet is punted to the RP.
- If the GRE header contains options, the packet is dropped silently.
- If the GRE packet is an invalid one (for example, no matching GRE tunnel record is found for this GRE packet), the packet is dropped silently.
- If the carrier IP header’s protocol field indicates any other protocol other than GRE, it is not a GRE packet. The packet is punted to the RP.
- If the packet is a GRE packet and has fragments, the packet is punted to the RP.
- If the payload in the GRE packet has options, the packet is punted to the RP.
- If the payload in the GRE packet has fragments, the packet is punted to the RP.
- If the payload for this GRE packet has fragments but is not destined for this router, the packet is forwarded.
- If the TTL of the payload is less than or equal to 1, the packet is punted to the RP.

Benefits

Router Performance

GRE tunneling on an E2 POS tunnel server card provides an aggregate throughput of approximately 2.7 Mpps of tunnel traffic. Also, ingress and egress line cards can run any feature loads that a customer requires.

Restrictions

Performance of Other Tunnel Protocols Impacted

GRE tunneling does not impact the performance of the normal IP forwarding path on the Cisco 12000 series Internet router. The performance of other IP tunnel protocols (UTI raw, FR UTI, and so on) is, however, affected if they run at the same time because they share the bandwidth that is available on the tunnel server card. A maximum of 2.7 Mpps of traffic is supported on the tunnel server card.

Scalability

- You can specify a maximum of 128 unique IP interfaces as GRE tunnel sources on a Cisco 12000 series Internet router.
- Each unique GRE bound IP interface can have a maximum of 500 tunnels destined to it.
- The Cisco 12000 series Internet router supports up to a maximum of 500 GRE tunnels.

Related Features and Technologies

- Cisco Express Forwarding (CEF)

Related Documents

- *Cisco IOS Release 12.0 Configuration Fundamentals Configuration Guide*
- *Cisco IOS Release 12.0 Configuration Fundamentals Command Reference*
- *Cisco Express Forwarding Overview*
- *Configuring Cisco Express Forwarding*
- *Cisco IOS IP and IP Routing Configuration Guide*

Supported Platforms

On a Cisco 12000 series Internet router, the following line cards support GRE tunneling on customer-facing interfaces:

- Engine 0
  - 1-Port OC-12 POS
  - 2-Port Channelized OC-3/STM-1 (DS1/E1)
  - 6-Port Channelized T3 (T1)

- Engine 2
  - 8-Port OC-3 POS
  - 16-Port OC-3 POS
  - 4-Port OC-12 POS
  - 4-Port OC-12 POS Revision B
  - 1-Port OC-48 POS
  - 1-Port OC-48 POS Revision B
  - 3-Port Gigabit Ethernet
  - 1-Port OC-48 DPT
  - 1-Port OC-48 DPT Revision B

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

Table 1 shows how the GRE Tunneling feature conforms to existing standards.

Table 1 RFC Compliance for GRE Tunneling on Cisco 12000 Series Internet Routers

RFC	RFC Function	GRE Tunneling on Cisco 12000 Series Internet Routers
RFC 1701	No options	Microcode contains hardware fast datapath
	Key	Not supported
	Checksum process	Not supported
	Sequence number	Not supported
	Source routing	Not supported
	Strict source routing	Not supported
RFC 2784	Key	Not supported
	Checksum process	Not supported
	Sequence number	Not supported
RFC 2890	Key	Not supported
	Checksum process	Not supported
	Sequence number	Not supported

Prerequisites

This section describes the prerequisites for using GRE tunneling on Cisco 12000 series Internet routers.

Dedicated Line Card Required

In order for a GRE tunnel on a Cisco 12000 series Internet router to come up, a Cisco 1-port OC-48 POS line card (tunnel server card) must be installed.

Software Requirements

GRE tunneling on a Cisco 12000 series Internet router requires Cisco IOS 12.0(21)S software or later versions.

Configuration Tasks

See the following sections for configuration tasks for GRE tunneling on a Cisco 1-port OC-48 POS line card in a Cisco 12000 series Internet router. Each task in the list is identified as either required or optional.

- Configuring the Tunnel Server Card (required)
- Configuring a GRE Tunnel (required)
- Configuring the ToS Byte (optional)
- Verifying GRE Tunnel Configuration (required)

Configuring the Tunnel Server Card

To configure a Cisco 1-port OC-48 POS line card as the dedicated tunnel server card:

	Command	Purpose
Step 1	`Router(config)# configure interface`	Enters interface configuration mode.
Step 2	`Router(config-if)# interface pos slot/port`	Selects an interface on the POS line card.
Step 3	`Router(config-if)# ip unnumbered loopback number` or `Router(config-if)# ip address {ip-address	mask}`	Configures the interface on the line card as IP capable. Because it is not necessary to advertise the IP address, you can enter the address of an unused private address space. If the interface is to be marked as IP unnumbered, it is recommended that you use a loopback interface, such as the tunnel source loopback.
Step 4	`Router(config)# hw-module slot slot-number mode server`	Configures the E2 POS line card in the specified slot as the dedicated tunnel server card.

Configuring a GRE Tunnel

To configure a GRE tunnel:

	Command	Purpose
Step 1	`Router(config)# configure interface`	Enters interface configuration mode.
Step 2	`Router(config-if)# interface tunnelnumber`	Selects the tunnel interface to be used for GRE tunneling.
Step 3	`Router(config-if)# tunnel mode gre ip`	Sets the encapsulation mode of the tunnel interface to GRE.
Step 4	`Router(config-if)# tunnel sourcename`	Specifies the name of the loopback interface used as the tunnel interface’s source address. The source address is the router where traffic is received from the customer network.
Step 5	`Router(config-if)# tunnel destination address`	Sets the IP address of the destination of the tunnel interface. The destination address is the router which transfers packets into the receiving customer network.
Step 6	`Router(config-if)# ip address address`	Sets the IP address of the tunnel interface.

Configuring the ToS Byte

You can optionally configure the ToS byte of the tunnel's IP header. If you do not specify a ToS byte, the three most significant bits (IP precedence bits) of the payload IP header are copied to the corresponding bits of the tunnel's carrier IP header.

To configure the ToS byte used in IP packet headers:

Command	Purpose
`Router(config-if)#` **`tunnel tos`** ***`number`***	Sets the value of the ToS byte. Valid values: 0 - 255. The three most significant bits of the ToS byte are called the IP precedence bits. Most applications and vendors currently support setting and recognizing these three bits. Example: To set an IP precedence value of 5 critical, you need to set the highest three bits of the ToS byte with a binary value of 10100000 (which is equivalent to the decimal value of 160 needed in the command value).

Verifying GRE Tunnel Configuration

Step 1 Use the **show running-config interface tunnel** command to display the tunnel destination IP address for interfaces.

```
Router(config)# show running-config interface tunnel 4
Current configuration : 165 bytes
!
interface Tunnel4
 ip address 7.7.7.7 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 tunnel source Loopback1
 tunnel destination 61.61.61.61
end
```

Step 2 Use the **show ip route** command to verify the IP routes are valid. There should be a valid entry for the tunnel destination address.

```
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, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set

     61.0.0.0/32 is subnetted, 1 subnets
S       61.61.61.61 [1/0] via 3.3.3.4
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, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set
```

```
     61.0.0.0/32 is subnetted, 1 subnets
S       61.61.61.61 [1/0] via 3.3.3.4
```

Step 3 Use the **show interface tunnel** command to verify that the tunnel interface is up.

```
Router(config)# show interface tunnel 4

Tunnel1 is up, line protocol is up
Hardware is Tunnel
  Internet address is 7.7.7.7/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 71.71.71.71 (Loopback1), destination 61.61.61.61
  Tunnel protocol/transport GRE/IP, sequencing disabled
  Tunnel TTL 255
  Key disabled
  Checksumming of packets disabled
  Last input 00:00:06, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6675 packets input, 457768 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     6787 packets output, 627804 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuration Examples

This section provides an example of how to create a GRE tunnel on the Cisco 12000 series Internet router:

```
Router# configure interface
Router(config)# interface pos 4/0
Router(config-if)# ip unnumbered loopback 45
Router(config-if)# exit
Router(config)# hw-module slot 4 mode server
Router(config)# interface loopback 45
Router(config-if)# ip address 100.0.2.1 255.255.255.0
Router(config-if)# exit
Router(config)# interface tunnel20
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source loopback 45
Router(config-if)# tunnel destination 100.10.2.4
Router(config-if)# ip address 10.1.1.1
Router(config-if)# tunnel tos 200
```

Note The IP address of the loopback 45 interface and the IP address (100.1.1.1) specified by the tunnel’s interface **ip address** subcommand must be different.

Command Reference

This section documents commands that are now supported on the Cisco 12000 series Internet router. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **hw-module slot mode server**
- **interface tunnel**
- **ip address**
- **show interface tunnel**
- **show running-config interface tunnel**
- **tunnel destination**
- **tunnel mode gre ip**
- **tunnel source**
- **tunnel tos**

hw-module slot mode server

To identify the card in a specified slot as a tunnel server card, use the **hw-module slot mode server** command in configuration mode. To disable the card as a tunnel server card, use the **no** form of this command.

hw-module slot *slot-number* **mode server**

no hw-module slot *slot-number* **mode server**

Syntax Description

number	Configures the E2 line card in the specified slot as the dedicated tunnel server card.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Usage Guidelines

This command identifies the card in the specified slot as a tunnel server card. This command is mandatory to enable GRE tunneling on the Cisco 12000 series Internet router.

Examples

The following example specifies the card in slot 2 as the tunnel server card:

```
Router(config)# hw-module slot 2 mode server
```

interface tunnel

To configure a GRE tunnel on the E2 tunnel server card, use the **interface tunnel** command in configuration mode to specify the tunnel in the Cisco 12000 series Internet router to be used for GRE tunneling. To disable the tunnel interface configuration, use the **no** form of this command.

interface tunnel*number*

no interface tunnel*number*

Syntax Description

number	Number of the tunnel to use. This is a logical value used to identify the tunnel interface.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Examples

The following example selects tunnel 4 for GRE tunneling:

```
Router(config)# interface tunnel4
```

ip address

To configure the IP address of the customer-facing tunnel interface with its logical tunnel number, use the **ip address** command in configuration mode. To disable the configuration of the destination address, use the **no** form of this command.

ip address *address mask* [**secondary**]

no ip address *address mask* [**secondary**]

Syntax Description

address	IP address of the local customer facing interface.
mask	Network mask used to identify a local customer facing interface.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Examples

The following example configures the customer-facing interface specified with the **tunnel source** command with the IP address 100.1.0.1 and a subnet mask 255.255.255.0:

```
Router(config-if)# ip address 100.1.0.1 255.255.255.0
```

show interface tunnel

To display the operational state of a GRE tunnel on the tunnel server card, use the **show interface tunnel** command.

show interface tunnel *number*

Syntax Description

number	Number of the GRE tunnel configured with the **interface tunnel** command.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Examples

The following example displays the operational status of GRE tunnel number 4:

```
Router(config)# show interface tunnel 4

Tunnel1 is up, line protocol is up
Hardware is Tunnel
  Internet address is 6.6.6.6/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 61.61.61.61 (Loopback1), destination 71.71.71.71
  Tunnel protocol/transport GRE/IP, sequencing disabled
  Tunnel TTL 255
  Key disabled
  Checksumming of packets disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5645250126 packets output, 462862434540 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

show running-config interface tunnel

To display the destination IP address configured for the customer-facing interface of a GRE tunnel, use the **show running-config interface tunnel** command.

show running-config interface tunnel *number*

Syntax Description

number	Number of the GRE tunnel configured with the **tunnel source** command.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Examples

The following example displays the configuration of GRE tunnel number 4:

```
Router(config)# show running-config interface tunnel 4
Current configuration : 165 bytes
!
interface Tunnel4
 ip address 7.7.7.7 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 tunnel source Loopback1
 tunnel destination 61.61.61.61
end
```

tunnel destination

To configure the destination address of a GRE tunnel, use the **tunnel destination** command in interface configuration mode. To disable the configuration of the destination address, use the **no** form of this command.

tunnel destination *address*

no tunnel destination *address*

Syntax Description

address	IP address of the destination of the GRE tunnel.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Examples

The following example configures the IP address 100.10.0.1 as the destination of a GRE tunnel:

```
Router(config)# tunnel destination 100.10.0.1
```

tunnel mode gre ip

To set the encapsulation mode of an interface on the tunnel server card to GRE over IP, use the **tunnel mode gre ip** command in interface configuration mode. To disable the tunnel interface, use the **no** form of this command.

tunnel mode gre ip

no tunnel mode gre ip

Syntax Description

None

Defaults

GRE tunneling

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Examples

The following example sets the encapsulation mode of tunnel 20 to GRE over IP:

```
Router(config)# interface tunnel 20
Router(config-if)# tunnel mode gre ip
```

tunnel source

To configure the local customer-facing interface of a GRE tunnel, use the **tunnel source** command in interface configuration mode. To disable the interface configuration, use the **no** form of this command.

tunnel source*name*

no tunnel source*name*

Syntax Description

name	Name of a loopback interface to use as the source address for packets in the tunnel. Maximum number of source loopback addresses that you can configure on a Cisco 12000 series Internet router: 128.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Examples

The following example configures the local interface “loopback1” as the ingress interface of a GRE tunnel:

```
Router(config)# tunnel source loopback1
```

tunnel tos

To configure the ToS byte in IP headers of packets that pass through the interface to the GRE tunnel, use the **tunnel tos** command in interface configuration mode. To disable the interface configuration, use the **no** form of this command.

tunnel tos *number*

no tunnel tos *number*

Syntax Description

number	ToS value. Valid values: 0 - 255.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.

Examples

The following example configures the ToS byte of IP headers in packets that are sent over the interface to 255:

```
Router(config)# tunnel tos 255
```

Glossary

ACL—Access control list.

ATM—Asynchronous Transfer Mode.

CEF—Cisco Express Forwarding.

GRE—Generic Routing Encapsulation. A standards-based tunneling protocol that can encapsulate a wide variety of protocol packet types inside tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork (RFC 1701 [5], RFC 1702 [6]).

GSR—Gigabit Switched Router. Former name of the Cisco 12000 series Internet router.

IP—Internet protocol.

LC—Line card.

Mpps—Million packets per second.

POS—Packet over Sonet.

PPP—Point-to-Point protocol.

pps—Packets per second.

PSA—Packet Switching ASIC. The ASIC on the performance OC48 line card that does the “fast path” packet forwarding operations.

RP—Route processor.

ToS—Type of service. A field in the IP header.

TSC—Tunnel server card. A dedicated card to do all the tunnel encapsulation and decapsulation work.