Tunnel ToS

Feature History

Release	Modification
12.0(17)S	This feature was introduced.
12.0(17)ST	This feature was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This document describes the Tunnel Type of Service (ToS) feature and includes the following sections:

Feature Overview

The Tunnel ToS feature allows you to configure the ToS and Time-to-Live (TTL) byte values in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. The Tunnel ToS feature is supported on Cisco Express Forwarding (CEF), fast switching, and process switching forwarding modes.

Tunneling and Tunnel Interfaces

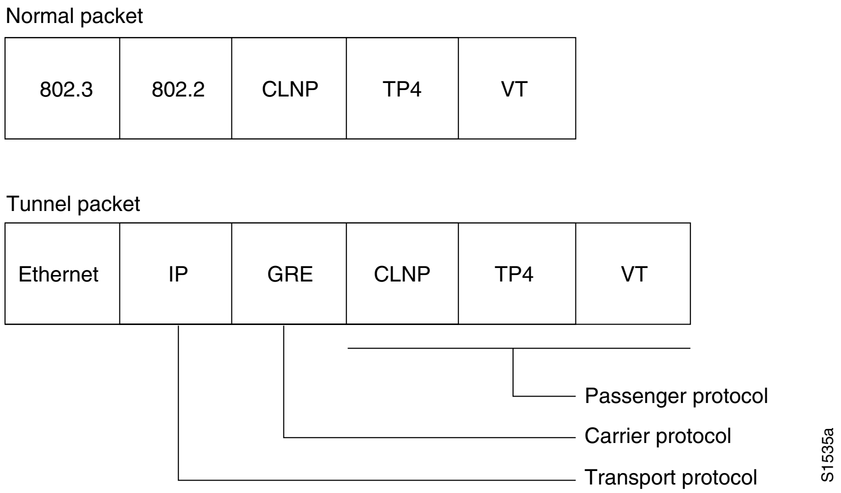
Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol. This feature is implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface is an architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. It is not tied to specific “passenger” or “transport” protocols. Because tunnels are point-to-point links, you must configure a separate tunnel for each link.

Tunneling has the following three primary components:

- Passenger protocol, which is the protocol that you are encapsulating (AppleTalk, Banyan VINES, CLNS, DECnet, IP, or IPX)
- Carrier protocol, which is one of the following encapsulation protocols:
  - Generic Routing Encapsulation (GRE), RFC2784
  - Cayman, a proprietary protocol for AppleTalk over IP
  - EON, a standard for carrying CLNP over IP networks
  - NOS, an IP-over-IP protocol compatible with the popular KA9Q program
  - Distance Vector Multicast Routing Protocol (DVMRP)
  - IP in IP, RFC2003
- Transport protocol, which is the protocol used to carry the encapsulated protocol (IP only)

Figure 1 illustrates IP tunneling terminology and concepts.

Figure 1 IP Tunneling Terminology and Concepts



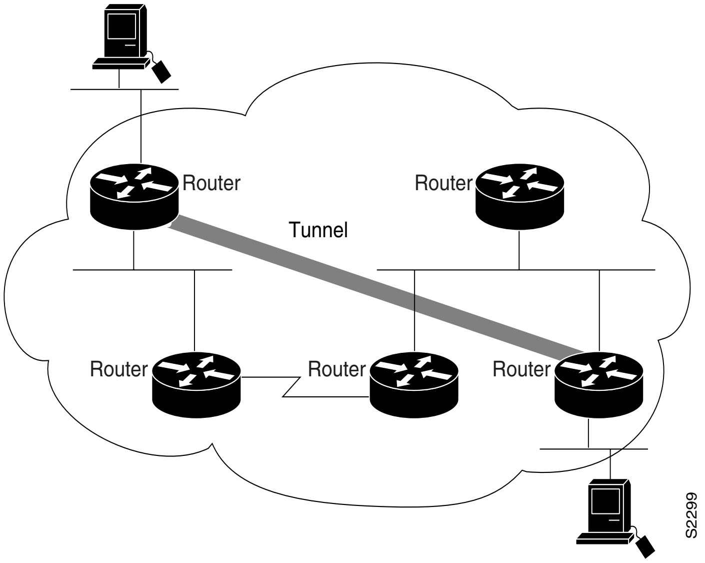
To understand the process of tunneling, consider connecting two AppleTalk networks with a non-AppleTalk backbone, such as IP. The relatively high bandwidth consumed by the broadcasting of Routing Table Maintenance Protocol (RTMP) data packets can severely hamper the backbone's network performance. This problem can be solved by tunneling AppleTalk through a foreign protocol, such as IP. Tunneling encapsulates an AppleTalk packet inside the foreign protocol packet, which is then sent across the backbone to a destination router. The destination router then removes the encapsulation from the AppleTalk packet and, if necessary, routes the packet to a normal AppleTalk network. Because the encapsulated AppleTalk packet is sent in a directed manner to a remote IP address, bandwidth usage is greatly reduced. Furthermore, the encapsulated packet benefits from any features normally associated with IP packets, including default routes and load balancing.

Advantages of Tunneling

The following are several situations in which encapsulating traffic in another protocol is useful:

- To provide multiprotocol local networks over a single-protocol backbone.
- To provide workarounds for networks containing protocols that have limited hop counts; for example, AppleTalk (see Figure 2).
- To connect discontinuous subnetworks.
- To allow virtual private networks across WANs.

Figure 2 Providing Workarounds for Networks with Limited Hop Counts



If the path between two computers has more than 15 hops, they cannot communicate with each other, but it is possible to hide some of the hops inside the network with a tunnel.

Special Considerations for Configuring Tunnel Interfaces

The following are considerations and precautions to observe when you configure tunneling:

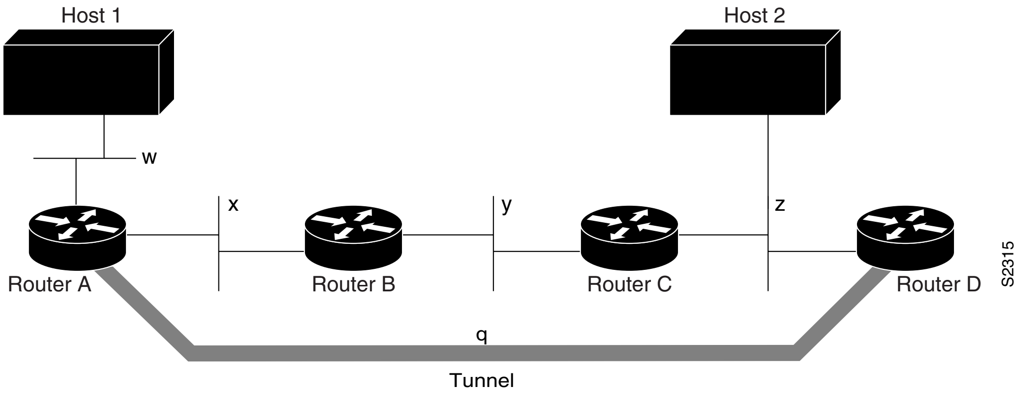
- Encapsulation and the removal of encapsulation at the tunnel endpoints are slow operations; in general, only processor switching is supported. However, fast switching of GRE tunnels was introduced in Cisco IOS Release 11.1 for the Cisco 2500 series and the Cisco 4000 series of routers, and CEF switching of GRE tunnels was introduced in Cisco IOS Release 12.1.
- Consider security and topology issues. Be careful not to violate access control lists. You can configure a tunnel with a source and destination that are not restricted by firewall routers.
- Tunneling might create problems with transport protocols that have limited timers (for example, DECnet) because of increased latency.
- Be aware of the environments across which you create tunnels. You might be tunneling across fast FDDI rings or through slow 9600-bps phone lines; some passenger protocols function poorly in mixed media networks.
- Multiple point-to-point tunnels can saturate the physical link with routing information.

- Routing protocols that make their decisions based solely on hop count will often prefer a tunnel over a multipoint real link. A tunnel might appear to be a one-hop, point-to-point link and have the lowest-cost path, but may actually cost more. For example, in the topology shown in Figure 3, packets from Host 1 will travel across networks w, q, and z to get to Host 2 instead of taking the path w, x, y, z because it "appears" shorter.
- A problem will occur if routing information from the tunneled network mixes with the information about the transport network. In this case, the best path to the "tunnel destination" is via the tunnel itself. This is called a recursive route and will cause the tunnel interface to shut down temporarily. To avoid recursive routing problems, keep passenger and transport network routing information disjointed:
  - Use a different AS number or tag.
  - Use a different routing protocol.
  - Use static routes to override the first hop (but watch for routing loops).

  If you see line a protocol down, as in the following example, it might be because of a recursive route:

```
%TUN-RECURDOWN Interface Tunnel 0
temporarily disabled due to recursive routing
```

Figure 3 Tunnel Precautions: Hop Counts



Benefits

The Tunnel ToS feature allows you to tunnel your network traffic and group all your packets in the same specific ToS byte value, as well as set the TTL hop-count value on those tunneled packets.

Restrictions

The ToS and TTL byte values are defined in RFC 791. RFC 2474 and RFC 2780 obsolete the use of the ToS byte as defined in RFC 791. RFC 791 specifies that bits 6 and 7 of the ToS byte (first two least significant bits) are reserved for future use and should be set to 0. Currently, the Tunnel ToS feature does not conform to this standard and allows you to set the whole ToS byte value, including bits 6 and 7, and decide which RFC standard to conform the ToS byte of your packets.

Related Documents

For more information on configuring tunnel interfaces, refer to the “Configuring Logical Interfaces” chapter in the *Cisco IOS Interface Configuration Guide*, Release 12.2.

- *Cisco IOS Interface Command Reference*, Release 12.2
- *Cisco IOS Interface Configuration Guide*, Release 12.2

Supported Platforms

In Cisco IOS Releases 12.0(17)S, 12.0(17)ST, and 12.2(8)T, the Tunnel ToS feature is supported on the following platforms:

- Cisco 805 ISDN, Serial, and IDSL Router
- Cisco 820 series of Business-class DSL routers
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1750 router
- Cisco 1751 router
- Cisco 2600 series Modular Access servers
- Cisco 3620 router
- Cisco 3640 router
- Cisco 3660 router
- Cisco 7100 series VPN routers
- Cisco 7200 series
- Cisco 7500 series
- Cisco RPM
- Cisco uBR 920 series Cable Access routers
- Cisco uBR 925 Cable Access router
- Cisco uBR 7200 series Universal Broadband routers
- Cisco 12000 Internet router

In Cisco IOS Release 12.2(14)S, the Tunnel ToS feature is supported on the following platforms:

- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series

Determining Platform Support Through Cisco Feature Navigator

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

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco 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 found at this URL:

http://www.cisco.com/register

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

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

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, 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 found at this URL:

http://www.cisco.com/register

RFCs

- RFC 791, *Internet Protocol*
- RFC 2472, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2780, *IANA Allocation Guidelines for Values in the Internet Protocol and Related Headers*

Configuration Tasks

See the following sections for configuration tasks for the Tunnel ToS feature. Each task in the list is identified as either required or optional.

- Specifying the Tunnel Interface (required)
- Configuring the Tunnel Source (required)
- Configuring the Tunnel Destination (required)
- Configuring the Tunnel ToS Byte Value (optional)
- Configuring the Tunnel TTL Hop-Count Value (optional)

Specifying the Tunnel Interface

To specify a tunnel interface and enter interface configuration mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`interface tunnel`** *`number`*	Creates tunnel interface if it does not exist and enters interface configuration mode.

Configuring the Tunnel Source

To configure the source address for the tunnel interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **`tunnel source`** `{`*`ip-address`* `|` *`type number`*`}`	Configures the tunnel source.

Note You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create multiple loopback interfaces and set the tunnel source as the loopback interface addresses.

Configuring the Tunnel Destination

To configure the destination for the tunnel interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# tunnel destination {hostname | ip-address}`	Configures the tunnel destination.

Configuring the Tunnel ToS Byte Value

To configure the ToS byte value for the tunnel interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# tunnel tos tos-byte`	Configure the ToS byte value for a tunnel interface.

Configuring the Tunnel TTL Hop-Count Value

To configure the TTL hop-count value for the tunnel interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# tunnel ttl hop-count`	Configures the TTL hop-count value for a tunnel interface.

Monitoring and Maintaining Tunnel Interfaces

To monitor and maintain ToS tunnels, use the following EXEC command:

Command	Purpose
`Router # show interfaces tunnel number`	Lists tunnel interface information.

Configuration Examples

This section provides the following configuration example:

- Tunnel ToS Example

Tunnel ToS Example

The following example shows how to specify the ToS byte value and TTL hop-count value for a tunnel interface:

```
interface tunnel 1
 tunnel tos 18
 tunnel ttl 128
```

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **show interfaces tunnel**
- **tunnel tos**
- **tunnel ttl**

show interfaces tunnel

To list tunnel interface information, use the **show interfaces tunnel** command in privileged EXEC mode.

show interfaces tunnel *number* [**accounting**]

Syntax Description

number	Port line number.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(17)S	Added tunnel ToS byte field to the command output.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Examples

The following is sample output from the **show interface tunnel** command:

```
Router# show interfaces tunnel 1

Tunnel4 is up, line protocol is down
  Hardware is Routing Tunnel
  Internet address is 10.1.1.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec)
  Tunnel source 9.2.2.1, destination 6.6.6.2
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TOS 0xF, Tunnel TTL 128
  Checksumming of packets disabled, fast tunneling enabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy, fifo
  Output queue 0/0, 1 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second 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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

Table 1 describes significant fields shown in the display.

Table 1 show interfaces tunnel Field Descriptions

Field	Description
Tunnel is {up | down}	Interface is currently active and inserted into ring (up) or inactive and not inserted (down). On the Cisco 7500 series routers, gives the interface processor type, slot number, and port number.
line protocol is {up | down | administratively down}	Shows line protocol up if a valid route is available to the tunnel destination. Shows line protocol down if no route is available, or if the route would be recursive.
Hardware	Specifies the hardware type.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method is always TUNNEL for tunnels.
loopback	Indicates whether loopback is set or not.
Keepalive	Indicates whether keepalives are set or not.
Tunnel source	IP address used as the source address for the tunnel packets.
destination	IP address of the tunnel destination.
Tunnel protocol	Tunnel transport protocol (the protocol the tunnel is using). This is based on the **tunnel mode** command, which defaults to GRE.
key	(Optional) ID key for the tunnel interface.
sequencing	(Optional) Indicates whether the tunnel interface drops datagrams that arrive out of order.
Last input	Number of hours, minutes, and seconds (or never) since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds (or never) since the last packet was successfully transmitted by an interface.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are displayed.

Table 1 show interfaces tunnel Field Descriptions (continued)

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Three asterisks (***) indicate the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
30 second input rate, 30 second output rate	Average number of bits and packets transmitted per second in the last 30 seconds. The 30 second input and output rates should be used only as an approximation of traffic per second during a given 30 second period. These rates are exponentially weighted averages with a time constant of 30 seconds. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of them medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver’s ability to handle the data.

Table 1 show interfaces tunnel Field Descriptions (continued)

Field	Description
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This usually is the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). Some collisions are normal. However, if your collision rate climbs to around 4 or 5 percent, you should consider verifying that there is no faulty equipment on the segment and/or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Number of times that the controller was restarted because of errors.

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to a serial interface.
show ip route	Displays all static IP routes or those installed using the AAA route download function.

tunnel tos

To configure the type of service (ToS) byte value for a tunnel interface, use the **tunnel tos** command in interface configuration mode. To use the payload ToS byte value (if payload protocol is IP) or 0, use the **no** form of this command.

tunnel tos *tos-bytes*

no tunnel tos

Syntax Description

tos-bytes	ToS byte value from 0 to 255 specified in the encapsulating IP header of a tunneled packet. The default value is 0.

Defaults

The default ToS byte value is the payload ToS byte value (if payload protocol is IP); otherwise, 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

If the **tunnel tos** command is not configured and the packet to be encapsulated is not an IP packet, the tunnel interface will use a default value of 0. If the **tunnel tos** command is not configured and the packet to be encapsulated is an IP packet, the tunnel interface will use the ToS byte value of the inner IP packet header.

Examples

The following example shows how to configure a ToS byte value of 55 on tunnel interface 1:

```
interface tunnel 1
 tunnel tos 55
```

Related Commands

Command	Description
show interfaces tunnel	Lists tunnel interface information.
tunnel ttl	Configures the TTL hop-count value for a tunnel interface.

tunnel ttl

To configure the Time-to-Live (TTL) hop-count value for a tunnel interface, use the **tunnel ttl** command in interface configuration command. To use the payload TTL value (if payload protocol is IP) or 255, use the **no** form of this command.

tunnel ttl *hop-count*

no tunnel ttl

Syntax Description

hop-count	TTL hop-count value from 1 to 255 to be used in the encapsulating IP header of a tunneled packet. The default is 255.

Defaults

The TTL default hop-count value is 255.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Examples

The following example shows how to configure a TTL hop-count value of 200 on tunnel interface 1:

```
interface tunnel 1
 tunnel ttl 200
```

Related Commands

Command	Description
show interfaces tunnel	Lists tunnel interface information.
tunnel tos	Configures the ToS byte value for a tunnel interface.