Generic Routing Encapsulation (GRE) Tunnel Keepalive

Feature History

Release	Modification
12.2(8)T	This feature was introduced on several platforms. The **keepalive** command was modified to make it available for use on tunnel interfaces.
12.2(14)S	This feature was integrated into Release 12.2(14)S.

This document provides configuration guidelines for deploying the GRE Tunnel Keepalive feature in Cisco IOS Release 12.2(14)S. It includes the following sections:

Feature Overview

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated generic routing encapsulation (GRE) tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel, or from just one side.

Benefits

The functionality of the **keepalive** command has been expanded to provide you with the ability to take down the line protocol of the GRE tunnel interface if the far end becomes unreachable.

Related Documents

For more information about tunnels, refer to these documents:

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

Supported Platforms

GRE tunnel keepalive packets are supported on the following platforms in Release 12.2(8)T:

- 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

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

- RFC 2784, *Generic Routing Encapsulation (GRE)*
- RFC 2890, *Key and Sequence Number Extensions to GRE*

Configuration Tasks

By default, keepalive packets are disabled on tunnel interfaces. To enable keepalive packets on an interface, use the **keepalive** command as illustrated in the tasks that follow. Each task in the list is identified as either required or optional.

- Configuring GRE Tunnel Keepalive (required)
- Verifying That Keepalive Packets Are Being Sent (optional)
- Troubleshooting Keepalive Packets (optional)

Configuring GRE Tunnel Keepalive

.To configure keepalive packets on tunnel interfaces, use the following commands beginning in privileged EXEC mode.

Command	Purpose
`Router# configure terminal`	Enters global configuration mode.
`Router(config)# interface tunnel` *number*	Enters interface configuration mode for the specified tunnel interface.
`Router(config-if)# keepalive` [*seconds* [*retries*]]	Enables keepalive packets on the interface and, optionally, specifies the time interval and the number of retries.
`Router(config-if)# exit`	Exits interface configuration mode.

Verifying That Keepalive Packets Are Being Sent

After you have enabled keepalive on the tunnel interface, you can use the **show interfaces** command to verify that keepalive packets are being sent.

```
Router# show interfaces tunnel 1
```

```
Tunnel1 is up, line protocol is up
  Hardware is 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 (5 sec), retries 4=====
  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 00:57:05, 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
     3 packets output, 1860 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Troubleshooting Keepalive Packets

Keepalive packets are GRE IP packets, so it is possible that they will be dropped somewhere between the GRE tunnel endpoints. To reduce the chance that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.

GRE keepalive packets may be sent from both sides of a tunnel, or from just one side. If they are sent from both sides, the period and retry parameters can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

Configuration Examples

This section includes the following configuration examples:

- Configuring Keepalive Packets on a Tunnel Interface Example
- Resetting Keepalive Values on a Tunnel Interface Example

Configuring Keepalive Packets on a Tunnel Interface Example

This example shows the configuration of a tunnel interface with the keepalive option set. The time interval for keepalive packets to be sent is 5 seconds; four attempts without response will be made (for a total of 20 seconds) before the protocol on the interface becomes inactive.

```
configure terminal
 interface tunnel1
  ip address 10.2.2.1 255.255.255.0
  load interval 30
  keepalive 5 4
```

```
  tunnel source 172.17.3.1
  tunnel destination 172.17.3.2
end
```

Resetting Keepalive Values on a Tunnel Interface Example

Using the same command sequence with different values changes the keepalive behavior on the same interface. The keepalive timeout value is set to 3 seconds, and the retry value is not specified. With these settings, the time out value has been reset to 3 and the retry option has been reset to the default of 3. Three consecutive (9 seconds) keepalives would need to lost before the tunnel1 interface would be disabled.

```
configure terminal
 interface tunnel1
  ip address 10.2.2.1 255.255.255.0
  load interval 30
  keepalive 3
  tunnel source 172.17.3.1
  tunnel destination 172.17.3.2
end
```

Command Reference

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

- **keepalive**

keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without response before bringing the tunnel protocol down for a specific interface, use the **keepalive** command in interface configuration mode. When the keepalive feature is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the **no** form of this command.

keepalive [*seconds* [*retries*]]

no keepalive [*seconds* [*retries*]]

Syntax Description

seconds	(Optional) Specifies the time interval, in seconds, at which keepalive packets are sent. Integer value greater than 0 and less than 32,767. The default is 10.
retries	(Optional) Specifies the number times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down. Integer value greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value had been specified previously, the default of 3 is used.

Defaults

seconds: 10 seconds
retries: 5

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The *retries* argument was added and made available on tunnel interfaces.
12.2(13)T	The default value for the *retries* argument was increased to 5.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(11)S.

Usage Guidelines

Default Behaviors

If you enter only the **keepalive** command with no arguments, defaults for both arguments are used.If you enter only the **keepalive** command and the timeout parameter, the default number of retries (5) is used.

And if you enter the **no keepalive** command, keepalive packets are disabled on the interface.

Keepalive Time Interval

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments down to 1 second. An interface is declared down after three update intervals have passed without receiving a keepalive packet unless the retry value is set higher.

Setting the keepalive timer to a low value is very useful for rapidly detecting Ethernet interface failures (transceiver cable disconnecting, cable not terminated, and so on).

Line Failure

A typical serial line failure involves losing Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

GRE keepalive packets may be sent from both sides of a tunnel, or from just one side. If they are sent from both sides, the period and retry parameters can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

Dropped Packets

Keepalive packets are treated as ordinary packets, so it is possible that they will be dropped. To reduce the chance that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.

Note When adjusting the keepalive timer for a very low-bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

GRE Tunnels with IPsec

When using GRE with IPsec, the keepalives are encrypted like any other traffic. As with user data packets, if the IKE and IPsec security associations are not already active on the GRE tunnel, the first GRE keepalive packet will trigger IKE/IPsec initialization.

Examples

The following example sets the keepalive interval to 3 seconds and the retry value to 7:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```